Office of Justice Programs

Privacy Impact Assessment
for the
Web Applications and Content Dissemination Platform Performance Measurement Tool (WACDP PMT) System

Issued by:
Maureen Henneberg

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

Date approved: September 30, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Office of Justice Programs (OJP) is required under the Government Performance and Results Act of 1993 (GPRA), Pub. L. 103-62; the GPRA Modernization Act of 2010, Pub. L. 111-352; the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, 2 C.F.R. § 200.329; and 31 USC 1116, Agency Performance Reporting, to collect performance measures data to demonstrate achievement of the agency's programmatic goals.

To measure program progress and success – and to assist OJP with fulfilling its responsibilities under the GPRA, Pub. L. 103-62; the GPRA Modernization Act of 2010, Pub. L. 111-352; and the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, 2 C.F.R. § 200.329 – applicants that receive funding from OJP must provide regular performance data. Performance measures are the data—specific values or characteristics—reported by grantees that measure the output or outcome of grantees' activities and services and demonstrate accomplishment of the goals and objectives of grant programs. These measures help capture inputs, outputs, and outcomes over time and enable pre- and post-comparisons that can be used to facilitate change as needed. These measures are defined in the grant solicitation and may be updated or revised during the life of the program.

The Web Applications and Content Dissemination Platform Performance Measurement Tool (PMT) is used to collect these performance measures and allows for access to the data through a range of standard reports. Funding recipients from five of OJP's grant-making components submit their performance data through PMT. The data collected through the PMT is frequently analyzed and presented in various reports and responses to information requests from across the Department of Justice and stakeholders. Additionally, in fiscal year 2020, the Bureau of Justice Assistance (BJA) began collecting death in custody data from the Edward Byrne Memorial Justice Assistance Grant (JAG) Program State Administering Agencies (SAAs) through the PMT. The Death in Custody Reporting Act (DCRA), Public Law 113-242, requires states that receive funding under the JAG Program to report to the Attorney General information regarding "the death of any person who is detained, under arrest, or is in the process of being arrested, is en route to be incarcerated, or is incarcerated at a municipal or county jail, State prison, State-run boot camp prison, boot camp prison that is contracted out by the State, or any State or local contract facility, or other local or State correctional facility (including any juvenile facility)."

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.

This Performance Measurement Tool (PMT) system collects and maintains the following information: names, contact information, performance information, race, sex, age, ethnicity, Unique Entity Identifier (UEI), and grant manager contact information to report performance measurement data on the progress and success of activities the agency funds. Within the BJA PMT, required information that is specifically collected for Deaths in Custody Reporting Act (DCRA) implementation includes the name, sex, race, ethnicity, year of birth, age of deceased as well as the date, time, location, description of circumstances and manner of death. The DCRA-related information also includes name and address information for the law enforcement agency that detained, arrested, or was in the process of arresting the deceased.

Under the umbrella of the PMT, there are six separate applications used by different OJP components:

- The OJP Performance Measurement Platform (PMP) is the user's single sign-on point of entry, performing user authentication for access to other PMT applications and managing user profiles.
- The Office for Victims of Crime Performance Measurement Tool (OVC PMT) that allows Federal Users, Partners, Grantees and Sub-Grantees to collect, review and report on performance measurement data.
- The Office of Juvenile Justice and Delinquency Prevention Data Collection and Technical Assistance Tool (OJJDP DCTAT) allows Federal Users, Grantees and Sub- Grantees to collect, review and report on performance measurement data.
- The Office of Juvenile Justice and Delinquency Prevention Compliance Management System, also referred to as Compliance Monitoring Tool (OJJDP CMT) provides a method for OJJDP to view compliance data by State/Territory, estimate missing data, track compliance rates, and report on compliance.
- The Bureau of Justice Assistance Performance Measurement Tool (BJA PMT) allows Federal Users, Grantees and Sub-Grantees to collect, review and report on performance measurement data.
- The Bureau of Justice Assistance Capacity Enhancement for Backlog Reduction and Post-Conviction Performance Measurement Tool (BJA PMT 2) allows Federal Users, Grantees and Sub-Grantees to collect, review and report on performance measurement data.

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. §§ 10110 (OJP), 10142 (BJA Director Duties), 11114 (OJJDP Administrator Duties), 20111 (OVC Director Duties), 60105 (Deaths in Custody Reporting); P.L. 103-62 (Government Performance and Results Act (GPRA)); P.L. 111-352 (GPRA Modernization Act of 2010); 2 C.F.R. § 200.329; 31 USC 1116 (Agency Performance Reporting).
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
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	First and Last Name
Date of birth or age	X	A, B, C & D*	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).
Place of birth	X	A, B, C & D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).
Sex	X	A, B, C & D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).

(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
Race, ethnicity, or citizenship	X	A, B, C & D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).
Religion	X	A, B, C & D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).
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			
Vehicle identifiers			
Personal mailing address	X	A, B, C, & D	PMP users have the option to create their user account using a personal email address, however OJP recommends use of business email address instead.
Personal e-mail address	X	A, B, C, & D	Email (OJP recommends use of work email, however some personal emails exist within the system), mailing address. PMP users have the option to create their user account using a personal email address, however OJP recommends use of business email address instead.
Personal phone number	X	A, B, C, & D	PMP users have the option to create their user account using a personal email address, however OJP recommends use of business email address instead.
Medical records number			

(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
Medical notes or other medical or health information	X	C and D	All programs EXCEPT DCRA collect aggregate group information only, without names or association to specific persons. DCRA collects health-related information on decedents. OJP protects this data from public disclosure based on the derivative privacy interest of survivors.
Financial account information			
Applicant information	X	A, B, C, & D	PMP users have the option of submitting either personal or business contact information, including phone, email, and physical address.
Education records	X	A, B, C, & D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).
Military status or other information	X	A, B, C, & D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).
Employment status, history, or similar information	X	A, B, C and D	All Programs EXCEPT DCRA collect only aggregate race/sex/age group information without association to names of any persons. DCRA collects personal information on decedents including names, dates of birth, sex, race, ethnicity, age at death and manner of death. OJP protects this data from public disclosure based on the derivative privacy interest of survivors (*See* National Archives & Records Administration v. Favish et al., 541 U.S. 157 (2004)).

(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
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	All programs include Congressionally- required proof of performance and compliance from grantees and subgrantees. Although it is unlikely that performance and disciplinary information would be submitted, PMT data may include employees' names and the work they are doing under the award that would not be retrievable by PII.
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	X	C & D	All programs EXCEPT DCRA include aggregate counts only (e.g., number arrested, tried, convicted, etc.). DCRA collects information on decedents' criminal records such as number of arrests and criminal history. OJP protects this data from public disclosure based on the derivative privacy interest of survivors.
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			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			

(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
- **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 created for accessing account may be maintained in system.
- **User passwords/codes**	X	A, B, C, & D	User IDs and passwords created for accessing account may be maintained in system.
- **IP address**			
- **Date/time of access**	X	A, B, C, & D	User IDs and passwords audit trails are different depending on the level of user accessing the system. Direct system access users (includes operating system level users, application server level users and database users) have different audit trails than privileged access users in the system.
- **Queries run**	X	A, B, C, & D	User IDs and passwords audit trails are different depending on the level of user accessing the system. Direct system access users (includes operating system level users, application server level users and database users) have different audit trails than privileged access users in the system.
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A & B	Training attendance and participation information for local and state law enforcement.

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			
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	
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	N/A	N/A	X	Internal OJP users (meaning staff members of DOJ and OJP technical assistance providers) have access to review the performance data provided by grantees.
DOJ Components	N/A	N/A	X	Internal OJP users (meaning staff members of DOJ and OJP technical assistance providers) have access to review the performance data provided by grantees.
Federal entities	N/A	N/A	X	External OJP users (e.g., law enforcement agency users) have access to submit performance data associated with the award.
State, local, tribal gov't entities	N/A	N/A	X	External OJP users (e.g., State or local government or tribal users) have access to submit performance data associated with the award.

Public	N/A	N/A	X	External OJP users (e.g., grantees and sub-grantees associated with an OJP grant or award or agreement users) have access to submit and performance data associated with the award.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	N/A	N/A	N/A	
Private sector	N/A	N/A	X	External OJP users (e.g., grantees and sub-grantees associated with an OJP grant or award or agreement users) have access to submit and performance data associated with the award.
Foreign governments	N/A	N/A	N/A	
Foreign entities	N/A	N/A	N/A	
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.

N/A

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.

Although PMT collects PII, the system is not a "system of record." That is, information in PMT cannot be retrieved by personally identifiable information as there are no fields specifically for collecting PII from the PMT data, including no retrievable audit data. There are, however, several free-form text/descriptive fields where PII data such as emails could be entered into the narrative. On occasion, a PMT user has entered PII into a field not meant for such, however this capture of incidental PII is exceedingly rare. OJP has evolving processes to filter unnecessary PII from entering into PMT and to the extent maintained, contain it to avoid accidental spillage. As to DCRA, OJP protects this data from public disclosure based on the derivative privacy interest of survivors.[1]

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

[1] Although the decedents' personal, health-related or other background information is collected and maintained in PMT, OJP does not retrieve the data collected in DCRA, in practice, by personal identifier.

collection or specific uses of their information? If no opportunities, please explain why.

There will be no opportunities for individuals to voluntarily participate in the use of data in PMT. The information in PMT cannot be retrieved by personally identifiable information; there are no fields specifically for collecting PII from the PMT data, including no retrievable audit data.

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 stated above, the PMT does not collect information retrievable by personally identifiable information. There are no records retrievable by PII about individuals so as to require amendments or corrections.

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):** June 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:** N/A
	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:** The actual elements of information within this system have been assigned a FIPS security categorization of Low, pursuant to the "high water mark" standard. This categorization is based on universal categorization of Moderate assessments in Confidentiality, Integrity, and Availability for both its Personal Identity and Authentication as well as its Official Information Dissemination Information Types.

X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** This system is subject to an annual internal assessment of OJP's defined Core Controls conducted throughout the course of the Fiscal Year. DOJ's annual Core Control assessment includes the testing and evaluation of the security and privacy controls safeguarding the information within the system. In addition, OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting this system 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:** OJP's applications have been integrated with the OJP Security Information & Event Management (SIEM) tool Splunk, which forwards logs to Splunk for auditing purposes. The audit trail captures any changes to the relevant users' data by DOJ personnel. OJP Cybersecurity teams monitor logs in accordance with DOJ security control requirements, which require monitoring on a weekly basis.
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**. All DOJ contracts that implicate PII, including contracts by which the Department obtains embedded contract personnel who process users' PII implicated by this system, are required under DOJ Acquisition Procurement Notice APN-21-07A to include the DOJ-02 Contractor Privacy Requirements clause, which satisfies the relevant requirements of the Privacy Act and other applicable law, regulation, and 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:** All Department personnel whose primary job responsibilities affect this system's users must complete relevant training.

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?

Access controls have been designed to preserve and protect PII. Role-based access is ensured in the system to minimize any role-based vulnerabilities. Password security has been implemented using OJP- specific complexity rules. PII in transmission is protected by usage of HTTPS (to ensure secure communication between users and the relevant website(s)), and TLS (Transport Security Layer) cryptographic protocol, version 1.2 or better.

Automated auditing of all information access types will be provided by the operating system and application software. Privacy risks are also minimized with physical controls. NTT Global Data Centers Americas houses the systems servers and infrastructure and has implemented physical security protocols to protect the business premises and information

systems from unauthorized access, damage, and interference.

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 5.7 "Administrative Management and Oversight Records" for records about administrative management activities in federal agencies.

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).

X 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:

This system does not constitute a "system of records" under the Privacy Act; thus, no further Privacy Act documentation is required.

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?

Most of the collected data is grantee or subgrantee performance measures and statistics and includes aggregate race/sex/age group information without association to names of specific persons, to minimize data collected for the purpose of reporting performance measurement data on the progress and success of funded activities.

- Data being collected:
  - Name, address, age, names, dates of birth, sex, race, ethnicity, phone/fax numbers, and email addresses.
- Sources of information:
  - Information collected from grantees and subgrantees.
- Specific uses:
  - The demographic information is used to report performance measurement data on the progress and accomplishment of activities the agency funds.
  - The demographics metadata is protected by both a security role (site manager) as well as via two-factor authentication.
  - DCRA related information will be examined and evaluated by Bureau of Justice Assistance (BJA) to determine which states are meeting the requirements for DCRA reporting and which states need assistance in doing so.

- Privacy Notice:
  - The DOJ Privacy Policy
- Decisions concerning security and privacy administrative, technical, and physical controls over the information:
  - 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. Data collection is minimized to only collect only data voluntarily.