Office for Access to Justice

Privacy Impact Assessment
for the
CLEAR Program System

Issued by:
Catalina Martinez, ATJ Senior Component Official for Privacy

Approved by: Christina Baptista, Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: [September 23, 2024]

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The system will host the information technology for the Civil Legal Empowerment, Access, and Reentry ("CLEAR") Program. As part of the CLEAR Program, ATJ will collaborate with the Federal Bureau of Prisons (FBOP) and a third-party partners, such as an academic institution or legal services provider, to provide civil legal services to incarcerated and formerly incarcerated individuals at selected FBOP facilities.

The CLEAR Program will include three segments: (1) developing and providing self-help materials to address civil legal needs of incarcerated and formerly incarcerated individuals; (2) conducting a series of empowerment workshops for incarcerated and formerly incarcerated individuals focused on family law, financial-related issues, and public benefits; and (3) creating a Medical Legal Partnership (MLP) with third-party partners to assist with pre-release Supplemental Security Income (SSI) mental health claims before the Social Security Administration (SSA). The system contains information on incarcerated and formerly incarcerated individuals, DOJ staff, third-party staff, and volunteers, such as medical records, custodial records, financial records, personal contact information, and recidivism-related data.

A Privacy Impact Assessment is being conducted because the CLEAR Program is a new program which will implicate, consistent with the eGovernment Act of 2002, information in identifiable form from the public. Additionally, consistent with the Paperwork Reduction Act, the CLEAR Program will involve the collection of information in identifiable form from 10 or more people.

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.

Through the CLEAR Program, ATJ aims to:

- Promote effective and impactful collaboration between medical and legal professionals, through a Medical Legal Partnership, that will help incarcerated individuals with severe mental health issues secure disability benefits, with the goal of reducing recidivism and improving access to housing and treatment.

- Educate and train the next generation of lawyers and doctors on how to work successfully with and best help incarcerated and reentering individuals with mental health disabilities.

- Understand and track the successes, barriers, and impact of the CLEAR Program, to inform the possible future scaling of the program.

The CLEAR Program is a partnership between ATJ, FBOP, and third-party partners. The sharing of information among all parties is essential to the success of the program. From the

contact information of those who will participate/volunteer, to the medical records from the incarcerated and formerly incarcerated individuals, the sharing of information between the parties is necessary to the fulfillment of the program.

The sources of the information are incarcerated and formerly incarcerated individuals participating in the program, the FBOP, past treatment providers of incarcerated and formerly incarcerated individuals (outside the FBOP), and students and staff of the third-party partners, such as an academic institution or legal services provider. Records from the incarcerated and formerly incarcerated individuals will be shared by FBOP to the third party representing the individuals. Then, the third party will share the records with ATJ so that ATJ staff can review and assist the legal/medical volunteers. The third party will share records gathered throughout the course of their representation with the SSA. ATJ will share contact information on third-party staff/volunteers with FBOP to enable the staff/volunteers to enter FBOP facilities to complete CLEAR Program tasks. However, FBOP and third-party staff will not have direct log-in access to any of ATJ's data.

Additionally, ATJ will be conducting surveys of incarcerated and formerly incarcerated individuals participating in the Empowerment Workshops and Medical Legal Partnerships to evaluate the effectiveness of the services provided by the CLEAR Program and how it should be scaled.

Information will be stored in electronic media in ATJ facilities via a configuration of personal computers, client/server, and mainframe systems, and/or federally-authorized cloud architecture and may be accessed by only ATJ staff. Specifically, ATJ will use DOJ laptops and SharePoint to maintain and process the data received. Information will be transmitted via encrypted e-mails and secured in SharePoint upon receipt. System logs are captured through Splunk and are maintained and reviewed by the Justice Security Operations Center (JSOC). Documentary (paper) records are maintained in manual file folders. At ATJ, information will only be shared with staff who are assisting with the CLEAR Program.

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	
Executive Order	
Federal regulation	28 CFR 0.33
Agreement, memorandum of understanding, or other documented arrangement	MOU between FBOP, ATJ, and third-party partners.
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 & C & D	Names of DOJ staff, incarcerated and formerly incarcerated individuals, and university students/third party staff
Date of birth or age	X	C & D	DOBs of incarcerated and formerly incarcerated individuals
Place of birth	X	C & D	Place of Birth of incarcerated and formerly incarcerated individuals
Gender	X	C & D	Gender of incarcerated and formerly incarcerated individuals, and university students/third-party staff
Race, ethnicity, or citizenship	X	C & D	Race, ethnicity, or citizenship of incarcerated and formerly incarcerated individuals, and university students/third-party staff
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C & D	SSN (full) of incarcerated and formerly incarcerated individuals
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C & D	Personal mailing address of incarcerated and formerly incarcerated individuals, and university students/third-party staff
Personal e-mail address	X	C & D	Personal e-mail address of incarcerated and formerly incarcerated individuals, and university students/third-party staff

(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 phone number	X	A & C & D	Personal cell phone number of DOJ staff, incarcerated and formerly incarcerated individuals, and university students/third party-staff
Medical records number	X	C & D	Medical records numbers of incarcerated and formerly incarcerated individuals
Medical notes or other medical or health information	X	C & D	Medical notes or other medical and health information for incarcerated and formerly incarcerated individuals
Financial account information	X	C & D	Financial account information for incarcerated and formerly incarcerated individuals
Applicant information	X	C & D	Applicant information for incarcerated and formerly incarcerated individuals, and university students/third-party staff
Education records	X	C & D	Education records for AICs, formerly incarcerated individuals, and university students
Military status or other information			
Employment status, history, or similar information	X	C & D	Employment status, history, or similar information for, incarcerated and formerly incarcerated individuals, and university students/third-party staff
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	Employment performance ratings or other performance information for incarcerated and formerly incarcerated individuals, and university students/third-party staff
Certificates			
Legal documents	X	C & D	Legal documents for incarcerated and formerly incarcerated individuals
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	Criminal records information for incarcerated and formerly incarcerated individuals
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			

(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
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**			
- **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:			System logs for DOJ laptops and SharePoint are captured via Splunk, however these logs are maintained and reviewed by the JSOC.
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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	X	Hard copy: mail/fax		Online	
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component		Other DOJ Components	X	Other federal entities	X
State, local, tribal		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): Third-party CLEAR program partners, such as academic institutions or legal services providers.					

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	ATJ staff working on the CLEAR Program share information via e-mail and access information via SharePoint.

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.**
DOJ Components	X	X		ATJ shares volunteer contact information with FBOP using (encrypted) Email. The information shared will grant volunteers access to FBOP facilities to complete CLEAR Program tasks.
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
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.

Not applicable.

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 Privacy Act Statement ((e)(3) notice) is provided when records are collected from individuals directly by ATJ and placed in a Privacy Act system of records, such as surveys of incarcerated and formerly incarcerated individuals participating in the Empowerment Workshops and Medical Legal Partnerships:

In accordance with 5 U.S.C. § 552a(e)(3), this Privacy Act Statement serves to inform you that the information on this form is collected pursuant to 28 CFR § 0.33. The primary purpose for soliciting this information is to allow FBOP, ATJ and the third-party partners to properly execute the CLEAR Program and provide civil legal services to incarcerated and formerly incarcerated individuals at selected FBOP facilities. The information provided may be used in accordance with the routine uses listed in the system of records entitled "Civil Legal Empowerment, Access, and Reentry (CLEAR) Program Records System, JUSTICE/ATJ-001" including to Members of Congress when they request information on behalf of an individual subject, to the General Services Administration and National Archives and Records Administration for records management inspections, to the U.S. Probation Office, to help individuals access Social Security disability benefits, for civil or criminal law enforcement purposes, for judicial or administrative proceedings which may be made available to the news media or the public, to another federal agency for a related-personnel matter or the performance of official business, to others working on an assignment to accomplish an agency function, to the White House for activities related to official or ceremonial duties of the President, to others as mandated by federal statute or treaty, or as necessary to respond to a security incident or breach. DOJ system of records notices can be found on the DOJ website at: https://www.justice.gov/opcl/doj-systems-records. Providing this information is voluntary. However, failure to provide this information may prevent you from being able to fully participate in all aspects of the CLEAR Program.

ATJ is in the process of publishing a SORN entitled "Civil Legal Empowerment, Access, and Reentry (CLEAR) Program Records System, JUSTICE/ATJ-001" that is designed to cover the records from this program and provide general notice of collection along with this PIA.

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.

Participation in the CLEAR Program is completely voluntary. However, failure to provide certain information may prevent the incarcerated or formerly incarcerated participant from being able to fully participate in all aspects of the CLEAR Program. For example, Individuals participating in the CLEAR MLP must provide information necessary to determine eligibility for SSI and as necessary to complete SSI applications. ATJ receives this information, as needed to determine eligibility to participate in and to manage the MLP program, from the third-party partners, who obtain it directly from the individual. The third-party partners obtain written consent from the individual participants to receive information about them from FBOP and to share their information with ATJ.

Surveys are administered to individuals who participate in the CLEAR Empowerment Workshops. The surveys are completely voluntary and refusal to complete the survey does not impact the participants ability to participate in the workshop or any other aspect of the CLEAR Program.

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.

The information in the system includes Privacy Act records covered by the ATJ-001 SORN, which includes access, amendment, and correction procedures for covered 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).

	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): **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:**
X	**This system is not subject to the ATO processes.** The CLEAR program will utilize DOJ issued GFE/laptops covered under the DOJ SDS End User Services (SEUS) ATO and the DOJ's instance of SharePoint and Outlook which is a part of the DOJ Email and Collaboration Services (ECS) ATO boundary. No other technology or systems will be utilized; thus, the program is not subject to the ATO process.
	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:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Information is only being sent to authorized personnel who have been trained on the proper use of DOJ information. They also sign the DOJ ROB which specifies what is and is not permissible use of DOJ data.
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:** All actions are logged via Splunk for DOJ laptops and SharePoint which are the sole vehicles for processing the CLEAR program information. Splunk performs near real time review of logs and identifies anomalous behavior which is sent to the JSOC.

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**.
	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: No additional training to the regular privacy training will be implemented.

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?

Information will be safeguarded in accordance with federal IT security requirements and DOJ's rules and policy governing automated information systems security, including physical security and access controls. These safeguards will include the maintenance of records and technical equipment in restricted areas, the use of encryption to protect data, and the required use of strong user authentication to access the system. Only those authorized personnel who require access to perform their official duties will be allowed to access the system equipment and the information in the system. The data will also be segregated and encrypted, and staff's ability to update inmate data will be restricted absent authorization.

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.)

Currently, the data is unscheduled to be destroyed. However, once the new retention schedule has been approved by NARA (which proposes a retention date of five years from the date that an individual's SSI application is filed) then documentary records will be destroyed by shredding; computer records will be destroyed by degaussing and/or shredding.

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:

ATJ is in the process of publishing a SORN entitled "Civil Legal Empowerment, Access, and Reentry (CLEAR) Program Records System, JUSTICE/ATJ-001" that is designed to cover the records from this program.

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?

There is a privacy risk associated with potential unauthorized access to the information. In order to mitigate this risk, ATJ utilizes technical and physical security controls such as access controls, encryption, and authentication requirements. Only those authorized personnel who require access to perform their official duties will be allowed to access the system equipment and the information in the system. The data will also be segregated and encrypted, and staff's ability to update program data will be restricted absent authorization.

There is a privacy risk associated with unauthorized dissemination of information, which is mitigated by security measures taken by third-party partners in storage and dissemination as well as encryption in transit.

There is a privacy risk associated with the overcollection of personal information, which is mitigated by making surveys anonymous where possible and limiting collection of data elements to those necessary to accomplish the purpose of the system.