Executive Office for Immigration Review

Privacy Impact Assessment
for
List of Pro Bono Legal Service Providers
(Pro Bono List)

Issued by:
Justine Fuga
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 25, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The primary mission of the Executive Office for Immigration Review (EOIR) is to adjudicate immigration cases by fairly, expeditiously, and uniformly interpreting and administering the Nation's immigration laws. To this end, EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings. EOIR is required to maintain a list, known as the List of Pro Bono Legal Service Providers ("List" or "Pro Bono List"), of organizations, pro bono referral services, and attorneys qualified under EOIR regulations to provide pro bono legal services in immigration proceedings (collectively referred to as "Providers"). Eligible organizations, referral services, and attorneys must apply to the agency to be included on the List. Through this application process, the agency collects applicant and Provider information such as: names; contact information; pro bono legal service descriptions; state and immigration court location where services are performed; alien registration numbers of individuals served; total hours and dates of pro bono services provided; declarations certifying the applicant's or Provider's eligibility; and public comments on application packages. EOIR updates the List quarterly, distributes copies of the List to its immigration courts and to the Department of Homeland Security (DHS), and posts the List on the EOIR public website. EOIR's Office of Policy (OP) administers this Pro Bono List program using two web-based applications, the internal-facing Pro Bono List Microsoft Dynamics System and the external-facing Pro Bono List User Portal. Because this program collects, uses, and disseminates personally identifiable information (PII), EOIR is conducting this privacy impact assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

Under Federal law, EOIR must maintain a List of Pro Bono Legal Service Providers that are willing to provide pro bono legal representation services to individuals who are in immigration proceedings before EOIR. *See* 8 U.S.C. §§ 1158(d)(4)(B), 1229(a)(1)(E)(ii) and (b)(2); 8 C.F.R. §§ 1003.61-1003.66. EOIR makes the List available to individuals in immigration proceedings,

updates the List quarterly, distributes copies of the List to EOIR's immigration courts and DHS, and posts the List on the EOIR public website.

Eligible organizations, referral services, and attorneys must apply to the agency to be included on the List. The eligibility requirements and procedures for placement on the List include at least 50 hours of pro bono legal services per year for each court's list on which a Provider appears (other than referral services), the applicant is not the subject of an order of disbarment or suspension under 8 C.F.R. § 1003.101, a public notice and comment period, and a three-year renewal period. There are also regulatory procedures for removing a Provider from the List.

Providers apply to be included on the List by completing and submitting the Form EOIR-56, Request to be Included on the List of Pro Bono Legal Service Providers for Individuals in Immigration Proceedings (OMB Control No. 1125-0015), or equivalent documentation, by mail, email, or online (via the Pro Bono List User Portal). EOIR collects the following information, including PII, through the initial and renewal application processes: names; contact information; EOIR ID numbers; pro bono service areas; specialties or restrictions on services provided; declarations regarding an applicant's or Provider's eligibility; alien registration numbers and dates and hours of service provided for clients in immigration proceedings as reported by the applicant or Provider in accordance with 8 C.F.R. § 1003.61 et seq.

Information collected includes biographic, contact and eligibility data supplied by nonprofit organizations, pro bono referral services, attorneys, and the public. Application packages include information such as names, addresses, and contact information (such as telephone and facsimile numbers, email addresses, and/or websites) of the applicants; declarations signed by the authorized officer of an organization, referral service, or attorney (used to assess eligibility for meeting/maintaining the requirements to be on the List); for attorneys and fully accredited representatives, the EOIR registration number (EOIRID), if any; for renewal applications, the name of the Immigration Court at which the Provider wishes to appear (initial and renewal applications), and rendered pro bono legal services for the prior three (3) years, including the alien registration numbers of clients (renewal applications).

Names of applicants are publicly posted so that members of the public may comment on the application for EOIR to consider in its decision on the application. A list of new applications is made publicly available prior to quarterly publication to facilitate the notice and comment period. Comments and complaints from the public are collected, maintained, and used to assess applicant eligibility.

An EOIR deciding official approves or denies applications. Decisions approving or denying applications are maintained and disseminated to applicants who are notified in writing of the decision. Denied applicants may apply again in the future.

If the application is approved, the Provider will be included on the List at the next quarterly update. The published List includes Provider names, contact information (including telephone and facsimile numbers as well as email addresses), and website address, if any. Copies of the List are disseminated both as electronic portable document files (PDFs) available online or as hardcopy printouts distributed to individuals in EOIR immigration proceedings or in DHS

custody. Providers may be voluntarily removed from the List at their own request. EOIR may also remove a Provider from the List for a variety of reasons (disbarred or suspended attorney, making a false declaration, fails to meet eligibility requirements, etc.). If the agency determines to remove a Provider from the List, the Provider will receive written notice and will be provided with an opportunity to respond and contest the determination. If removed from the List, the Provider's name and contact information will be removed from the List in the next quarterly update and the agency will send written confirmation to the Provider of such removal. All Providers with a pending application or currently listed must notify the agency within 10 business days of any changes to the Provider's contact information, specific limitations in providing pro bono services, or loss of eligibility.

EOIR OP uses a web-based system, the Pro Bono List Microsoft Dynamics System, to collect, track, and manage the application process, the List, and Provider information and documents. This system includes an external-facing web-based component, the Pro Bono List User Portal, which simplifies the application process for Providers. Through the Pro Bono List User Portal, members of the public may submit applications and update their contact information.

The system is connected to the EOIR eRegistry application and auto populates attorney or accredited representative information, such as EOIRID number and bar license information, for purposes of creating Portal user accounts and completing applications. Application packages submitted by mail or email are scanned and manually entered into the system by OP staff. Application packages are stored in the Dynamics System as well as on EOIR network drives. The system automatically generates a unique number to identify and track each application. The assigned deciding official reviews the application and reviewing attorneys working under their supervision may communicate with applicants via email to request additional information. For verification purposes, the deciding official will also use the Case Access System for EOIR (CASE) to retrieve information about clients served by Providers submitting renewal applications.

The Dynamics System is used alongside internal Microsoft Office 365 tools, such as Outlook, Word, Excel, and SharePoint, and agency network drives (on-premises and cloud-based). Program staff correspond with applicants via email in Microsoft Outlook. Deciding officials draft application decisions in Microsoft Word and sign them in Adobe Acrobat. The complete List and contact information for applicants and Providers are maintained by program staff using Microsoft Excel. Program records are stored in a configuration of on-premises servers, such as EOIR network drives, and cloud-based solutions, including the DOJ/EOIR Microsoft Azure Gov Cloud.

Only authorized EOIR personnel may access the internal components of the Dynamics System and associated network drives and cloud storage. Program staff may only access the Dynamics System on approved DOJ devices after logging into EOIR's secured network and verifying their identity with multi-factor authentication. User permissions are tailored to the user's particular role and for official purposes.

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	8 U.S.C. §§ 1158(d)(4)(B), 1229(a)(1)(E)(ii) and (b)(2).
Executive Order	
Federal regulation	8 C.F.R. §§ 1003.61-.66, 1240.10(a)(2), 1240.11(c)(1)(iii), 1240.32(a), 1240.48(a), and 1241.14(g)(3)(i).
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, C, D	Names of EOIR personnel; Names of applicants and Providers (USPER and non-USPER); Names of clients served by Providers (USPER and non-USPER); Names of public commenters (USPER and non-USPER)
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
Religion			

(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
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C, D	Alien registration numbers (A-numbers) of clients served by Providers (USPER and non-USPER)
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address, e-mail address, phone number	X	C, D	Personal mailing address, email address, and phone number of applicants and Providers (USPER and non-USPER) if used by the applicant or Provider as their business contact information; Address, phone number, and email address of public commenters (USPER and non-USPER)
Business mailing address, e-mail address, phone number	X	C, D	Business mailing address, email address, and phone number of applicants and Providers (USPER and non-USPER); Business mailing address, email address, and phone number of public commenters (USPER and non-USPER)
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	C, D	EOIRID numbers and bar license information of attorneys or accredited representatives authorized to practice before EOIR (USPER and non-USPER). Unique applicant numbers are assigned to individuals and organizations (USPER and non-USPER) to identify and track each application.
Education records			
Military status or other 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
Employment status, history, or similar information	X	C, D	Type of Provider (non-profit organization, pro bono referral service, private attorney), type of application (initial or renewal), immigration court location where applicant intends to provide pro bono services, specialties or limitations on pro bono services, hours and dates of pro bono services provided, declaration under penalty of perjury regarding sufficiency of applicant's or Provider's eligibility.
Employment performance ratings or other performance information, e.g., performance improvement plan			
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, D	Proof of organization's non-profit status.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			

(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
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	C, D	Signature of authorized officer or attorney (USPER and non-USPER) authorized to act on behalf of the organization certifying the applicant's or Provider's eligibility for inclusion on the List.
- **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, C, D	User ID of authorized EOIR personnel and members of the public (USPER and non-USPER) accessing the system.
- **User passwords/codes**	X	A, C, D	User password of authorized EOIR personnel and members of the public (USPER and non-USPER) accessing the system.
- **IP address**	X	A, C, D	IP address of authorized EOIR personnel and members of the public (USPER and non-USPER) accessing the system.
- **Date/time of access**	X	A, C, D	Date/time of access, user activity, date/time of user activity of authorized EOIR personnel and members of the public (USPER and non-USPER) accessing the system.
- **Queries run**			
- **Contents of files**			

(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
Other (please list the type of info and describe as completely as possible):	X	C, D	EOIR may receive other categories of PII from members of the public (USPER and non-USPER) commenting on applications or in complaints submitted by members of the public regarding an applicant or Provider. Though not solicited by EOIR, applicants and Providers may disclose other categories of PII to EOIR throughout the course of the application, renewal, or removal process.

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	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		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			Relevant information is provided on a case-by-case basis to: EOIR's Attorney Discipline Program or Fraud and Abuse Prevention Program, if needed to investigate a violation of the rules of professional conduct for immigration practitioners representing clients in EOIR immigration proceedings, or if the application package indicates a potential violation of law; EOIR's Freedom of Information Act (FOIA) Unit if necessary to respond to a FOIA or Privacy Act request.
DOJ Components	X			EOIR may share relevant information with other DOJ components articulating an authorized need to know the information to perform official duties. For instance, EOIR may share information with the United States Attorneys' Offices and the Civil Division for an authorized litigation need.

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			EOIR provides DHS with copies of the quarterly List to comply with the statutory obligation to provide information about the availability of pro bono legal services for applicants seeking asylum and related relief. EOIR may also share relevant information with other federal entities in accordance with the law and regulation.
State, local, tribal gov't entities	X			On a case-by-case basis for an authorized law enforcement or court litigation need.
Public	X			EOIR shares information with members of the public upon request pursuant to the Freedom of Information Act (FOIA) or the Privacy Act (PA), subject to applicable exemptions. EOIR publishes the Pro Bono List on its website, which is available to members of the public. Additionally, EOIR makes available on its public website, for public comment prior to publication, the list of pending qualified applicants to be placed on the Pro Bono List.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			If determined relevant to judicial proceedings or otherwise required by law or court order, information in the system may be shared with counsel, parties, witnesses, and courts or other judicial tribunals for litigation purposes.
Private sector				
Foreign governments				
Foreign entities				

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.**
Other (specify):	X			Members of the public or other entities may obtain information from EOIR in the following ways: pursuant to a FOIA request; pursuant to publicly available information on the EOIR website; pursuant to a written authorization or consent provided by the subject of a record maintained by EOIR.

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.

EOIR publicly publishes the List of Pro Bono Legal Service Providers on its website (https://www.justice.gov/eoir/list-pro-bono-legal-service-providers). This List is also available through data.gov, (https://catalog.data.gov/organization/doj-gov?_publisher_limit=0&publisher=Executive+Office+for+Immigration+Review). The List contains each Provider's name, address, other relevant contact information, and any specialties or limitations on the services provided. EOIR is required by law to identify representatives available to provide pro bono representation in immigration proceedings. EOIR protects the privacy of each Provider's information by only publishing on the List the minimum amount of information necessary to fulfill the agency's legal obligations to identify available pro bono representatives.

Section 5: Notice, Consent, Access, and Amendment

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

EOIR publishes the complete pro bono application process on its website (https://www.justice.gov/eoir/list-pro-bono-legal-service-providers), which informs individuals about how EOIR collects, uses, shares, and otherwise processes PII as part of this process. EOIR

also employs several other methods to notify and inform individuals about how the agency collects, uses, shares, and processes their PII: (1) SORNs published in the Federal Register and available for convenience on the DOJ website (https://www.justice.gov/opcl/doj-systems-records#); (2) Privacy Act § 552a(e)(3) notices displayed on the Form EOIR-56 and on the Pro Bono List User Portal; and (3) the DOJ Privacy Policy, displayed on the common footer of the EOIR website (https://www.justice.gov/doj/privacy-policy).

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.

Members of the public, specifically, organizations and attorneys, voluntarily provide nearly all the information in the system. Individuals seeking initial or continued inclusion on the Pro Bono List have an opportunity to participate in the collection of information when they submit their application materials. Applicants and Providers may decline to provide certain information to EOIR; however, a deficient application package may hinder the determination process and could impact the applicant's or Provider's eligibility to be included on the Pro Bono List.

Comments from the public are also collected, maintained, and used to assess the suitability of applicants' and Providers' inclusion on the List. Commenters are required to provide an exact copy of the comment to the applicant or Provider, who will have an opportunity to respond to unfavorable comments. Commenters may request copies of application packages for inspection, and applicants or Providers do not have the opportunity to consent to such dissemination of their information because the disclosure is required by regulation. 8 C.F.R. § 1003.63(f)(1) (". . . upon request a copy of each application shall be made available for public review.").

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.

Applicants and Providers may access their own application packages and determinations in the Pro Bono List User Portal, with the ability to update their own contact information.

Otherwise, individuals may submit a FOIA request or a PA access or amendment request with EOIR's FOIA Office. Consistent with 28 C.F.R. §16.46, requests to access records must be in writing and should be addressed to the EOIR Office of the General Counsel, 5107 Leesburg Pike, Suite 2150, Falls Church, VA 22041, EOIR.FOIARequests@usdoj.gov. The envelope and letter should be clearly marked "Privacy Act Access Request." The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request must include a general description of the records sought and must include the requester's full name, current address, and place and date of birth. The request must be signed and either notarized or submitted under penalty of perjury. Instructions for making Privacy Act requests electronically through the Public Access Link (PAL), a public facing portal, are available on the EOIR website (https://www.justice.gov/eoir/freedom-

information-act-foia). To access and submit requests through PAL, individuals must set up a user account with a unique username and password. After registering for a PAL account, users can submit a Privacy Act request, check the status of the request, and download records.

EOIR primarily relies on applicants and Providers to contact the agency to update its records and maintain the integrity of EOIR's records. Alternatively, individuals may request correction or amendment of records pertaining to them in the Pro Bono List Program Records in accordance with procedures set forth under the Privacy Act (5 U.S.C. § 552a(d)(2)-(4)). Individuals seeking to contest or amend information maintained in the system should direct their requests to the Office of the General Counsel stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. An individual who is the subject of a record in this system may seek amendment of those records that are not exempt. A determination of whether a record is exempt from amendment 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	**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 the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** The Pro Bono List is within the JCON eWorld – Adjudication Support ATO, most recently granted Aug. 29, 2025, expiring Aug. 29, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **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:** There are no outstanding POAMs for any privacy controls.
	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 information or information 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 NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: EOIR has assigned a FIPS 199 security categorization of Moderate.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** In accordance with DOJ Order 0908, *Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information*, and to protect EOIR's data from spills, leaks, and/or misuse, EOIR performs daily monitoring of cybersecurity incidents, continuously evaluates alerts for cyber threats, and conducts annual cybersecurity incident response testing.
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:** EOIR collects and maintains audit logs for 120 days and reviews audit logs weekly to ensure compliance with security and privacy standards.
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**.
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:** Training is administered to all EOIR personnel authorized to use the system to ensure EOIR personnel know how to properly use the system and information contained therein. To ensure new personnel understand how to properly use the system, OP provides new personnel with copies of written procedures and training demonstrations of the system.

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?

EOIR personnel and members of the public accessing the system require authorized user accounts with role-based permissions that limit the extent to which user groups access, view, edit, download, send, and receive information, including PII. EOIR requires Portal users to obtain a verified user account and authenticates user identities before EOIR grants access to its public-facing applications. For EOIR personnel, access is only granted to those with a need to know the information, who have obtained the requisite clearance, who have completed annual

cybersecurity and privacy awareness trainings, and who annually review and sign the DOJ IT Rules of Behavior. Role-based access controls allow the system administrator to grant access to information based on a least privilege access setting. Access and user permissions are tailored to the particular user's role and need for the information. Role-based access controls additionally ensure data is handled, retained, and disposed of appropriately. User identities are verified with each log in attempt using multi-factor authentication. EOIR employs DOJ Login to authenticate user identities to prevent unauthorized access, and DOJ Login automatically deactivates EOIR user accounts with more than 90 days of inactivity. User accounts are locked for specified periods of time after a specified number of unsuccessful log-in attempts. Additionally, EOIR OIT monitors user accounts daily for suspicious activity.

EOIR regularly monitors and audits user activity to detect suspicious activity. EOIR has established minimum auditable events based on DOJ IT security requirements that the information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when and where it occurred, the source of the event, outcome of the event, and identity of any user or subject associated with the event. In addition, system administrators have access to the audit logs that display user access and roles. Logs are collected in real time and reviewed weekly to determine what users have accessed, added, modified, downloaded, or disposed of information in the system. Generally, authorized Pro Bono List Program staff can access all records in the system, but there are limitations on editing certain types of records depending on the user's role. The Pro Bono List User Portal is publicly accessible through the internet; however, Portal users only have access to their own information/applications and do not have the ability to directly access any other data or records stored in the system.

Several other virtual and physical security measures are also in place to safeguard information, such as IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and audit logs. EOIR conducts regular vulnerability scanning and configuration management activities. EOIR's databases are stored on fully secured servers, maintained in compliance with the Federal Information Security Modernization Act (FISMA) and the Office of Management and Budget (OMB) guidance. System data and records, including information stored in associated network drives, are backed up regularly and stored according to applicable record retention schedules and policies. Consistent with FISMA and the National Institute of Standards and Technology (NIST) security controls, transmissions of EOIR non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (SFTP), or Secure Sockets Layer (SSL) encryption.

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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

The records in this system are subject to the Pro Bono Representative Files records schedule (DAA-0582-2016-0001). All records in this system are temporary records. The quarterly Lists

are cutoff each quarter, maintained until the end of the calendar year, and destroyed 4 years thereafter (DAA-0582-2016-0001-0001). Application files are cutoff at the end of the calendar year in which the applicant or Provider was removed from the List or in which the applicant was rejected or disapproved, transferred to inactive status one year after cutoff, and destroyed three years after the cutoff date (DAA-0582-2016-0001-0002 and -0003).

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:

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (Jul. 14, 2021), https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

EOIR will be publishing a new SORN covering Pro Bono List Program Records.

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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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,***
- ***Type of technology employed (e.g. AI/ML),***

- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

There is a risk that the system inadvertently collects more information than may be necessary. Applicants may submit more information than necessary for EOIR to process an application. To avoid overcollection of information, EOIR recommends applicants use the Form EOIR-56. This Form is designed to elicit the minimum information needed by EOIR to process the application and is reviewed regularly for this purpose. EOIR also provides a Privacy Act Notice on the Form EOIR-56 and through the Pro Bono List User Portal to remind applicants and Providers that they voluntarily provide their information to EOIR.

While ease of access through the Pro Bono List User Portal creates convenience for applicants or Providers to submit application packages and access and update their own information, it simultaneously offers ease of access for unauthorized users if access is not carefully monitored. Similarly, EOIR must carefully monitor internal access and use of Pro Bono List information and records by EOIR personnel. Improper use or access by EOIR personnel poses potential threats to privacy, including unauthorized access to the information, compromised integrity of the information, and improper use, disclosure, or disposal of the information. EOIR carefully monitors internal and external access in a variety of ways as described in Section 6.

There are privacy risks associated with EOIR's disclosure of applicant and Provider information, including PII. EOIR is required by law to identify eligible pro bono legal service providers. To identify such Providers, EOIR makes available on its public website the complete List with Provider contact information. EOIR mitigates privacy risks by only publishing limited PII as necessary to comply with legal obligations to maintain and disseminate the List. Therefore, the published List includes only the minimum information necessary for an individual to identify and contact an eligible Provider for purposes of inquiring about or obtaining the Provider's services.

EOIR also publishes the names of all pending qualified applicants to be placed on the List for public comment, and members of the public may review each application, in accordance with 8 C.F.R. § 1003.63(f). EOIR mitigates privacy risks associated with publicly disseminating application packages during the comment period in several ways: (1) applicants are notified in advance that information on initial applications will be disclosed to the public for comment prior to adjudication of the initial application; (2) EOIR only provides copies of application packages if specifically requested; (3) EOIR does not disclose client information that may be included in the application package and will redact such information before providing copies for public inspection; and (4) EOIR limits the public comment and inspection period to only 15 days.