Executive Office for Immigration Review

Privacy Impact Assessment
for the
Recognition and Accreditation System

Issued by:
Alexander Hartman
Senior Component Official for Privacy

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

Date approved: March 18, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the 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 Executive Office for Immigration Review (EOIR) adjudicates immigration cases of noncitizens who are in removal proceedings. The purpose of the Recognition & Accreditation (R&A) Program is to authorize qualified non-attorneys ("accredited representatives") to provide representation in immigration matters through approved organizations ("recognized organizations"). The R&A Program will be administered through a conglomerate of information-collecting systems, collectively, the Recognition and Accreditation System (R&A System).

The R&A System is a full scope computer-based program that will substantially automate the R&A Program application and review process. This system is comprised of three components: (1) R&A Database (RAD); (2) R&A Access (RAA); and (3) TransUnion TLOxp. The R&A Database is an internal-facing Microsoft Dynamics application that allows authorized users to enter, search for, and process recognition and accreditation applications. R&A Access is a public facing web-based application to be used by applicants to electronically submit their R&A applications and supporting materials. Through an online portal for RAA, a recognition or accreditation applicant will submit to EOIR the relevant applications, R&A Forms EOIR-31 (Request for New Recognition, Renewal of Recognition, Extension of Recognition of a Non-Profit Religious, Charitable, Social Service, or Similar Organization (OMB#1125-0012)) and EOIR-31A (Request by Organization for Accreditation or Renewal of Accreditation of Non-Attorney Representative (OMB#1125-0013)), along with supporting materials. TransUnion TLOxp is a web-based service that allows EOIR's Office of Security (OS) to conduct authorized background checks on each proposed representative.

Internally, the R&A System will shift all processing and review of the R&A Program applications to the substantially automated process, which will include processes that will require staff to verify the presence and sufficiency of all documentation necessary to demonstrate an individual's or organization's eligibility for admittance into the Program. Externally, the R&A System will allow applicants to submit their R&A applications electronically through RAA. Information collected through the portal, R&A forms, and supporting materials include, at a minimum: an applicant organization's name and contact information; a proposed representative's name, date of birth and contact information; licensing and education information of any attorneys at the organization; the proposed representative's criminal and financial records, if applicable; organizational chart; resumes for proposed representatives; and evidence of the organization's federal tax-exempt status from the Internal Revenue Service and of non-profit status from the state where the organization is registered.

All information and documents pertaining to a recognition or accreditation application used by EOIR to make a final disposition in each application will be housed in the R&A System. Additionally, the new process contemplates an online access feature to allow Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), as an entity legally authorized to review and comment on R&A applications, access to be able to upload, save, edit, digitally sign, and submit

documents online through the application, as well as view the application package that the organization submitted to EOIR.

EOIR's R&A Program partners with EOIR's OS to conduct background checks on each proposed representative using TransUnion TLOxp (https://tloxp.tlo.com/logout.php). The R&A Program extracts certain documents from accreditation applications and places these documents in a shared drive to which OS has access. OS obtains the documents from the shared drive and uses the information therein to run the background checks using TLOxp. The TransUnion TLOxp service enables OS to search accredited representatives and obtain a background check report (TLO report) on the individual. To generate a TLO report, OS enters the full name and date of birth for the applicant into the TransUnion TLOxp service. If this initial search does not return any results, OS will ask the individual for additional identifiers, typically a social security number or aliases/other names used by the individual. Each TLO report contains personal information about the individual, such as aliases used, known addresses, prior employers, criminal convictions, judgments, liens, etc. The report is retained in a shared drive only accessible to OS. After reviewing the TLO report, OS provides a written recommendation letter to the R&A program, which is saved in the individual's R&A file.

The new R&A system will maintain information from application packets and OS as is necessary to review and process recognition and accreditation requests of organizations and representatives. It will also house the information and digitized copies of previously received applications.

The information contained in application packets may be accessed internally by EOIR employees, as well as contractors, with approved access, who will be inputting information into the database and reviewing and processing application packets. The information in the system may also be shared with USCIS as required per 8 C.F.R. § 1292 to ensure that USCIS is given the opportunity to provide input on applications for recognition and accreditation. In addition, EOIR may share information in the R&A system with other agencies in accordance with routine uses set forth in EOIR System of Records Notices (SORNs) or as otherwise permitted by law and regulation.

EOIR also posts a R&A Roster of recognized organizations and accredited representatives on its public website, which is available to members of the public. The R&A Roster includes the following information: the recognized organization's name, address(es), and phone number(s); the date the organization received its recognition; the date the recognition is scheduled to expire; the current recognition status; the accredited representative's name; accreditation status, as either fully or partially accredited; and the date the accreditation is scheduled to expire.

This Privacy Impact Assessment addresses the privacy implications associated with the collection of information through the R&A system and the mitigations in place to protect individuals' personally identifiable information (PII).

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.

Under delegated authority from the Attorney General, EOIR adjudicates immigration cases of subjects who are in removal proceedings. Under the regulations, individuals appearing before the immigration court may represent themselves or be represented by practitioners, including accredited representatives from recognized organizations. *See* 8 C.F.R. §§ 1001.1(ff), 1292.1. The purpose of the R&A System is to improve efficiencies, accountability, and accuracy in the adjudication of applications for recognition and accreditation of organizations and representatives, and for the management of the R&A Program. It is engineered to serve as the primary record for recognition and accreditation applications from initial application to adjudication by EOIR and final disposition.

Presently, once EOIR receives an applicant organization's relevant information from the applications and supporting documents, EOIR staff enters said information into a mail log and a tracking log. The inefficient manual process associated with former R&A Program internal database (Recognition and Accreditation Database (RANDA)) necessitated that EOIR develop a new database (Recognition and Accreditation Database (RAD)) with automated processes. Internally, the system will shift substantially all processing and review of the R&A Program applications to the automated process, which will still include processes that will require staff to verify the presence and sufficiency of all documentation necessary to demonstrate an individual's or organization's eligibility for admittance into the Program. RAD will additionally allow EOIR to import data, to include digitized copies of previously received applications and supporting documents, from the network drive. EOIR will over time upload these files— applications and supporting documents—from the network drive into the current system. The new system will also house the information and digitized copies of previously received paper applications.

Additionally, through the public facing RAA portal, organization applicants seeking recognition and accreditation will be able to register to use RAA, log into the portal, and electronically submit their application packets and supporting materials. In turn, EOIR will have the ability to issue decisions through the system, send and receive notifications and periodic reminders, and run reports based on data in the different data fields. Notifications and periodic reminders may be sent, for example, from EOIR personnel to the point of contact of a recognized organization to alert the organization that its recognition will expire soon and that it needs to renew an application to stay current. PII in these notifications is limited to the name and email address of the EOIR personnel, the name and email address of the authorized officer point of contact for the organization, the name and email address of the accredited or proposed representative, IP address and system/admin data. The R&A System will house information submitted by applicant organizations for recognitions and accreditations.

The new process contemplates an online access feature that will enable USCIS, from whom EOIR receives electronic correspondence regarding organizations and representatives, access that will allow

USCIS to be able to upload, save, edit, digitally sign, and submit documents online through the application, as well as view the application package that the organization submitted to EOIR. Regulations require that USCIS be given the opportunity to provide input on applications for recognition and accreditation prior to EOIR's final determination. 8 C.F.R. § 1292 et seq.

In short, the R&A System will enable EOIR to collect and review information and documents supplied by organization applicants seeking recognition and accreditation, communicate with these applicants, and share information with USCIS. The records contained within the R&A System will be maintained to facilitate receiving and evaluating requests for recognition and accreditation, and to prepare any necessary reports.

This new R&A System is intended to facilitate an increased level of efficiency in processing applications for recognition and accreditation.

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. §§ 1103, 1229a, b(4), and 1362.
Executive Order	
Federal regulation	8 C.F.R. § 1292.1(a)(4), 3-5, 11, 12, 13(b), 14-18. 8 C.F.R. § 1001.1(j).
Agreement, memorandum of understanding, or other documented arrangement	Memorandum of Agreement Between the Department of Homeland Security and the Department of Justice Executive Office for Immigration Review Regarding the Sharing of Information of Immigration Cases (Oct. 22, 2012) ("2012 DHS MOA"). Addendum I: Adding U.S. Customs and Border Protection As A Signatory to the Memorandum of Agreement Between The Department of Homeland Security and The Department of Justice Office for Immigration Review Regarding the Sharing of Information on Immigration Cases (effective September 23, 2022) ("2022 DHS MOA Addendum").
Other (summarize and provide copy of relevant portion)	N/A

Section 3: Information in the Information Technology

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

Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	Agency employees working on R&A matters; USCIS employees responding to R&A matters; members of the public included in R&A matters.
Date of birth or age	X	C, D	Applicant for accreditation's date of birth.
Place of birth	X	C, D	Applicant for accreditation's place of birth if on resume or supporting documents.
Sex	X	C, D	Applicant for accreditation's sex if on resume, supporting documents, or background check results.
Race, ethnicity, or citizenship	X	C, D	Applicant for accreditation's citizenship if on resume or supporting documents.
Religion	X	C, D	Applicant for accreditation's religion if on resume or supporting documents.
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	Applicant for accreditation's SSN may be requested to complete background checks and is included in the background check results.
Tax Identification Number (TIN)	X	C, D	Organization's business tax ID numbers as part of tax-exempt information. Applicant for accreditation's tax ID number, if applicable, may appear in the background check results.
Driver's license	X	C, D	Results of background checks for accredited representatives may include driver's license numbers.
Alien registration number	X	C, D	Applicant for accreditation could include truncated A-number in supporting documents to establish relevant experience. Background check results may include alien registration number.
Passport number	X	C, D	Applicants for accreditation could include copies of their passports in supporting documents to establish identity and date of birth.

(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
Mother's maiden name			
Vehicle identifiers	X	C, D	Background check results may include vehicle identifiers of applicants for accreditation.
Personal mailing address	X	C, D	Results of background checks for accredited representatives may include personal mailing address, or if included on resume or supporting documents.
Personal e-mail address	X	C, D	Applicant for accreditation's personal e-mail address if on resume, supporting documents, or background check results.
Personal phone number	X	C, D	Applicant for accreditation's personal phone number if on resume, supporting documents, or background check results.
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	C, D	Background check results may include information about debts and liens of applicants seeking accreditation status. Organization's income, budget, fee schedules, fee waivers included as supporting documents.
Applicant information	X	C, D	Applicants seeking recognition or accreditation may voluntarily include such information not otherwise solicited by EOIR.
Education records	X	C, D	Applicant for accreditation's education records if on resume or supporting documents.
Military status or other information	X	C, D	Applicant for accreditation's military status if on resume or supporting documents.
Employment status, history, or similar information	X	C, D	Applicant for accreditation's employment status and history if on resume, supporting documents, or background check results.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C, D	Disciplinary information of applicants seeking accreditation may be included for character and fitness determination.
Certificates	X	C, D	Educational and licensing certificates of applicants for accreditation if on resume or supporting documents.

(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
Legal documents	X	C, D	Professional licenses, briefs and motions if included as supporting documents from accreditation applicants.
Device identifiers, e.g., mobile devices	X	C, D	Phone numbers of recognition and accreditation applicants will be included in application packet and may appear in background check results.
Web uniform resource locator(s)			
Foreign activities	X	C, D	Foreign educational and licensing information of accreditation applicants if on resume or supporting documents.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	Criminal history of applicant seeking accreditation may be included for character and fitness determination. Background check results may include criminal record of applicant.
Juvenile criminal records information	X	C, D	Criminal history of applicant seeking accreditation may be included for character and fitness determination. Background check results may include criminal record of applicant.
Civil law enforcement information, e.g., allegations of civil law violations	X	C, D	Immigration status of applicant seeking accreditation may be included for character and fitness determination. Background check results may include civil law enforcement information of applicants seeking accreditation status.
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information	X	C, D	Grand jury indictment records may be included for character and fitness determination.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	Applicants seeking to establish character and fitness may submit information concerning witnesses to demonstrate their suitability to represent clients.
Procurement/contracting records			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Proprietary or business information	X	C, D	Business information, to include bylaws, articles of incorporation, mission or purpose statement, may be included as supporting documents for organization seeking recognition. Background check results may include an applicant for accreditation's business affiliations.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			Background check results only produce photos if a person is possibly a fugitive. If the applicant seeking accreditation has a common name, a fugitive with a similar name could be associated with this applicant.
- **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:			Entity Data is Audited Access to Audit data is only available to System Administrator Roles in Dynamics
- **User ID**	X	A, B, C, D	User IDs for DOJ employees, contractors, and detailees may include PIV credentials.
- **User passwords/codes**	X	A, B, C, D	
- **IP address**	X	A, B, C, D	
- **Date/time of access**	X	A, B, C, D	
- **Queries run**	X	A, B, C, D	
- **Contents of files**	X	A, B, C, D	

(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	The free form fields in the system for notes and comments may include notations about name and address changes, changes in accreditation staff, or the date USCIS submitted a recommendation. Background check results may include other PII related to representatives seeking accreditation, such as licenses (e.g., hunting, fishing, pilot), weapons permit, voter registration, and property (e.g., deeds, foreclosures, and evictions).

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	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	X	Private sector	
Commercial data brokers	X				
Other (specify): TransUnion TLOxp is a commercial data broker, and EOIR uses this service to conduct background checks on applicants for accreditation for purposes of character and fitness determinations.					

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X	X	X	EOIR internally shares information with personnel who need to know the information to perform their job duties.
DOJ Components	X			EOIR may share information with other DOJ components articulating an authorized need to know the information. For instance, EOIR may share information with the United States Attorneys' Offices and the Civil Division for an authorized litigation need.
Federal entities	X	X	X	Pursuant to 8 C.F.R. § 1292 et seq, USCIS must be given the opportunity to provide input on recognition and accreditation applications; therefore, EOIR may share information relating to accreditation and recognition requests with USCIS. EOIR may also share information with other federal entities in accordance with the law, regulation, and/or Memoranda of Agreement.
State, local, tribal gov't entities	X			On a case-by-case basis for an authorized law enforcement or court 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.**
Public	X		X	EOIR shares information with members of the public upon request pursuant to the Freedom of Information Act (FOIA) or the Privacy Act, subject to applicable exemptions. EOIR also shares a R&A Roster of recognized organizations and accredited representatives on its website, which is available to members of the public. The R&A Roster provides contact information, accreditation and recognition status and the date the accreditation and recognition is scheduled to expire for all recognized organizations and accredited representatives. EOIR also sends determination letters electronically to organizations and their accredited representatives.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			EOIR may share information collected in the R&A system on a case-by-case basis pursuant to a FOIA request or Privacy Act litigation.
Private sector	X			Private sector individuals and entities may obtain information relating to recognized organizations and accredited representatives on EOIR's public website. Private sector individuals and entities may also obtain information relating to recognized organizations and accredited representatives pursuant to a FOIA request.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Foreign governments	X			Foreign governments may obtain information relating to recognized organizations and accredited representatives on EOIR's public website. Foreign governments may also obtain information relating to recognized organizations and accredited representatives pursuant to a FOIA request.
Foreign entities	X			Foreign entities may obtain information relating to recognized organizations and accredited representatives on EOIR's public website. Foreign entities may also obtain information relating to recognized organizations and accredited representatives pursuant to a FOIA request.
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 makes available to the public a report called the R&A Roster, which is a list of all currently approved recognized organizations and accredited representatives, on its website, under the R&A Program (https://www.justice.gov/eoir/recognition-accreditation-roster-reports). This roster is also available through data.gov. Before publication or dissemination, EOIR redacts most PII, with the exception of accredited representatives' contact information, which is minimally required to ensure access to legal representation for individuals appearing before EOIR. The R&A Roster includes the following information: the recognized

organization's name, address(es), and telephone number(s); the date the organization received its recognition; the date the recognition is scheduled to expire, and the current recognition status; the accredited representative's name; accreditation status, as either fully or partially accredited; and the date the accreditation is scheduled to expire.

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.

EOIR employs several methods to notify and inform individuals about how the agency collects, uses, shares, and processes their PII: (1) SORNs published in the Federal Register (see Section 7.2 of this PIA); (2) a Privacy Act statement displayed prior to an applicant's entry into RAA, pursuant to 5 U.S.C. § 552a(e)(3), (https://getaccredited.eoir.justice.gov/login), that informs users of the information collection; and (3) this Privacy Impact Assessment once published.

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 representatives, voluntarily provide nearly all the information handled by the R&A Program relating to accreditation and recognition requests. Applicant organizations and representatives may decline to provide certain information to the R&A Program; however, a deficient application packet may slow down the determination process and could impact their eligibility to obtain accreditation or recognition status.

Information is also received from USCIS and pursuant to any background checks. The organization and the individual seeking accreditation receive a copy of any recommendation issued by USCIS. If the R&A Program receives additional information from USCIS that is relied upon in the adjudication of a recognition or accreditation request, such information is also shared with the individual and/or organization at issue. As it relates to background checks, individuals seeking accreditation have an opportunity to participate in the collection of information when they complete Form EOIR-31A and submit their resume. Applicants do not receive copies of the background check report conducted by OS. However, applicants are given an opportunity to address any concerns that may arise during the background check.

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.

Individuals may obtain access to information in the R&A System in the following ways: (1) an Authorized Officer, who is the point of contact designated by each organization, may view and download applications and supporting documents submitted electronically by login to R&A Access portal; or (2) individuals may submit a Privacy Act 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 for recognition and accreditation 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 R&A System 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. Some information may be exempt from contesting record procedures. 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):** December 10, 2024, expiration date of December 10, 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:** The only outstanding POAM is the Records and Information Management Certification (RIMCert).
	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 Recognition and Accreditation System is categorized as 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*, EOIR performs daily monitoring of cybersecurity incidents, and conducts annual cybersecurity incident response testing and evaluation of alerts for cyber threats to safeguard and protect EOIR's data from spills and/or leaks.
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:** Audit logs are collected in real time and are reviewed weekly by the software development and IT security staff 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:** In addition to the annual DOJ cybersecurity and privacy trainings, EOIR requires personnel to complete records training and annually review and accept OIT Rules of Behavior to supplement its privacy- and cybersecurity-related trainings.

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

The R&A System currently uses role-based permissions to ensure data is handled, retained, and

disposed of appropriately. EOIR employs the Department's DOJ Login system to authenticate user identities to prevent unauthorized access, and DOJ Login automatically deactivates EOIR user accounts with more than 90 days of inactivity. Additionally, EOIR OIT monitors accounts daily for suspicious activity. EOIR employees must also complete Cyber Security Awareness Training, Privacy Training, Records Training, and sign the DOJ Rules of Behavior.

In addition, R&A 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, downloaded or deleted from the system. Generally, authorized users of the R&A system can access all records in the system, but there are limitations on editing certain types of records depending on the user's role.

The RAA portion of the R&A system is publicly accessible through the internet; however, RAA users only have access to their own information/applications, and do not have the ability to directly access any other data stored in the R&A system. Only authorized EOIR personnel have access to the data supplied by RAA users.

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 maintained in the R&A system are not currently scheduled and are therefore retained indefinitely. EOIR is in the process of drafting and obtaining NARA approval of new records schedules. Until the records retention schedule is completed, the records in the system will not be disposed of.

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/EOIR-001, Records and Management Information System, 69 FR 26179 (May 11, 2004), https://www.govinfo.gov/content/pkg/FR-2004-05-11/pdf/04-10564.pdf (EOIR is in the process of updating this SORN).

- JUSTICE/EOIR-003, Attorney Discipline System, 85 FR 32423 (May 29, 2020), https://www.govinfo.gov/content/pkg/FR-2020-05-29/pdf/2020-11528.pdf.

- JUSTICE/BIA-001, Decisions of the Board of Immigration Appeals, 48 FR 5331 (Feb. 4, 1983), https://www.justice.gov/opcl/docs/48fr5331.pdf (EOIR is in the process of updating this SORN).

- JUSTICE/BIA-002, Roster of Organizations and their Accredited Representatives Recognized by the Board of Immigration Appeals, 45 FR 75908 (Nov. 17, 1980), https://www.justice.gov/opcl/docs/45fr75908.pdf.

    - NOTE: JUSTICE/EOIR-004 Roster of Recognized Organizations and Accredited Representatives is currently under review by the Office of Privacy and Civil Liberties as of September 2024 and will replace BIA-002.

- 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.

Section 8: Privacy Risks and Mitigation

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

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

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

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the agency's official duties, particularly records that are unscheduled, is always a potential threat to privacy. The information housed in the R&A System is required for the R&A Program to process recognition and accreditation requests received by the office. EOIR's R&A Program only collects and receives information from organizations and representatives seeking recognition and accreditation to provide legal representation in immigration proceedings. This information is required to assess the suitability of applicants seeking to provide legal representation. When an applicant organization submits an application packet, there is an understanding that the R&A Program will only collect and disclose information and records as necessary to process and adjudicate the recognition or accreditation request. In order to

mitigate these risks, information and records maintained in the system are only collected and stored as a result of a specific request for information. Role-based access controls allow the system administrator to grant access to information based on a least privilege access setting. Moreover, system access is primarily granted to EOIR's R&A Program employees and contractors who complete the requisite security clearance and/or background check process, identity validation, and annual security and privacy training, and who annually review and acknowledge DOJ's Rules of Behavior to maintain system access.

b. Potential Threats Related to Use of the Information

Potential threats to privacy because of the agency's collection, use, and maintenance of the information in the R&A System include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information. EOIR mitigates these risks by only granting access internally to authorized EOIR personnel, or contractors, who have obtained the requisite clearance. Access to the system is role-based and internal agency users are only authorized to access information that they need to know to perform their job duties. Role-based access controls additionally ensure data is handled, retained, and disposed of appropriately. Training is administered to all system users before they gain access to the system. Finally, audits are conducted at regular intervals to ensure that there is no improper use by users. Auditing such data and making users aware of the detailed audit trail on every action in the system limits privacy and security risks. Additionally, EOIR personnel must complete Cyber Security Awareness Training, Privacy Training, and sign the DOJ Rules of Behavior.

c. Potential Threats Related to Dissemination

EOIR may share information collected in the R&A system internally within EOIR, when the disclosure is required by law or regulations, or on a case-by-case basis to respond to a request. EOIR has streamlined its processes to obtain consent from individuals to disclose their records by making available the Form EOIR-59, Certification and Release of Records, and Form DOJ-361, Certification of Identity. EOIR directs all requests for information to its Office of the General Counsel for review pursuant to laws and regulations governing information sharing and disclosure, such as FOIA and the Privacy Act.

EOIR may also share information with USCIS as regulations require that USCIS be given the opportunity to provide input on applications for recognition and accreditation prior to EOIR's final determination. Through R&A Access, USCIS will eventually have the ability to upload, save, edit, digitally sign, and submit documents online, as well as view application documents received by EOIR. Additionally, the R&A Program makes available on EOIR's public website a report of all currently approved recognized organizations and accredited representatives. This R&A Roster includes the following information: the recognized organization's name, address(es), and phone number(s); the date the organization received its recognition; the date the recognition is scheduled to expire; the current recognition status; the accredited representative's name; accreditation status, as either fully or partially accredited; and the date the accreditation is scheduled to expire.

Applicants may also be able to view and download only their own applications and supporting documents submitted electronically by login into R&A access. Before EOIR grants access to RAA, EOIR requires users to obtain a verified user account and authenticates user identities.

While unauthorized disclosures of PII are a possibility due to user error, EOIR mitigates risks by only granting internal access to employees or contractors who complete the requisite security clearance and/or background check process, identity validation, and annual security and privacy trainings, and who annually review and acknowledge DOJ's Rules of Behavior to maintain system access. Internal user accounts are reviewed regularly, and user activity audits are conducted regularly to monitor suspicious activity.

Several virtual and physical security measures are also in place to safeguard sharing of information, to include IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and audit logs. EOIR has established minimum auditable events based on DOJ IT security requirements demanding that the information system produces audit records with 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. EOIR's databases are stored on fully secured servers, maintained in compliance with FISMA and the Office of Management and Budget (OMB) guidance. Consistent with FISMA and 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.

Finally, Memoranda of Agreement (MOAs) and contracts provisions are in place to manage and control access to EOIR information by its partners and vendors. EOIR's current MOAs are described in Section 2.2 of this PIA. Contracts with vendors contain security language required by the DOJ, including contracts for FedRAMP-compliant cloud services, such as the Microsoft Azure Cloud supporting critical infrastructure for the R&A System. MOAs and contracts contain privacy and security provisions including confidentiality and need-to-know requirements, as well as breach response protocols and termination provisions for any failure to abide by these requirements.