Executive Office for Immigration Review

Privacy Impact Assessment
for the
Attorney Discipline System

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: April 15, 2026

(March 2025 DOJ PIA Template)

<u>Section 1</u>: 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. Under delegated authority from the Attorney General, EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings. Individuals and aliens who are subjects of EOIR immigration proceedings may be represented by counsel.

EOIR regulates the professional conduct of immigration practitioners in order to protect the public, preserve the integrity of immigration proceedings and adjudications, and maintain high professional standards among immigration practitioners. The EOIR Office of the General Counsel (OGC) serves as the agency's chief legal counsel on matters of immigration practitioner discipline and, through a Disciplinary Counsel, administers the Attorney Discipline (AD) Program. The AD Program investigates complaints involving alleged misconduct associated with practice before EOIR's immigration courts and the Board of Immigration Appeals (Board) to determine whether a practitioner has engaged in criminal, unethical, or unprofessional conduct.

The AD Program uses an internal web-based information system, hosted on a hybrid computing environment (on-premises and cloud-based solutions) to collect, process, investigate, and resolve complaints made to the Program. The AD System handles information related to the professional conduct of immigration practitioners and organizations and unauthorized practice of immigration law. This information includes but is not limited to names and contact information; complaints; evidentiary submissions and witness statements; investigative information; records and transcripts of underlying immigration proceedings affected by the alleged conduct; complaint dispositions; and records, transcripts, notices, orders, and decisions by EOIR adjudicators in formal disciplinary proceedings. EOIR may refer complaints and share relevant information with Federal, state, local, territorial, or tribal entities or authorities for further action, investigation, or prosecution. A list of currently and previously disciplined practitioners is publicly available on the EOIR website. EOIR may also share information in these systems for the routine uses described in applicable system of records notices (SORNs) or as otherwise permitted by law and regulation.

EOIR initially included the AD system in the 2018 PIA for the JCON eWorld General Support System (GSS). Since then, EOIR has reconceptualized the scope and boundaries of the JCON eWorld GSS, and the AD system has undergone significant changes: new types of information were added to the system; some on-premises components of the system were migrated to cloud-based components; new notification and reporting capabilities were added to the system; and the system was connected to the Case Access System for EOIR (CASE)[1] for purposes of querying relevant immigration case and proceeding information. Such changes present new privacy risks, necessitating this updated PIA.

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.

EOIR has the authority to impose disciplinary sanctions on practitioners and recognized organizations who violate rules of professional conduct in practice before the immigration courts and the Board. *See* 8 C.F.R. §§ 1003.1(d)(2)(iii), 1003.1(d)(5), 1003.101-.111, 292.3. The AD Program, led by a designated Disciplinary Counsel, protects the integrity of legal representation in immigration proceedings before EOIR by regulating the professional conduct of immigration practitioners and recognized organizations under 8 C.F.R. §§ 1003.0(f)(1), 1003.101-.111. The AD Program investigates alleged misconduct by immigration practitioners, makes referrals to disciplinary and law enforcement authorities in appropriate circumstances, issues warning letters, and initiates informal and formal disciplinary proceedings.

Generally, discipline of practitioners and recognized organizations is initiated by the filing of a complaint. Any individual may file a complaint about the conduct of a practitioner or recognized organization, including immigration judges, appellate immigration judges, the practitioner's clients, opposing counsel in EOIR proceedings, other practitioners, or members of the public. Practitioners also have an affirmative duty to self-report certain conduct, such as suspension or disbarment from the practitioner's state bar. Complaints and self-reports must be submitted in writing to the EOIR Disciplinary Counsel, and complainants are encouraged to use the Form EOIR-44, Immigration Practitioner/Organization Complaint Form (OMB No. 1125-0007). Complaints and self-reports should be as specific and detailed as possible to include relevant names, dates, location, or other details identifying the offending conduct or behavior, and supporting documentation should be provided if available. Complaints are submitted by mail or email to the AD Program.

When a complaint or self-report is filed, the AD Program conducts a preliminary investigation and depending on the findings may elect to: (1) take no further action; (2) issue a warning letter or informal admonition to a practitioner; (3) enter into an agreement in lieu of disciplining a

---

[1] CASE is an internal, web-based electronic case management system and database of immigration case information for the immigration courts and the Board, designed to internally manage all aspects of an immigration proceeding and serving as the official data repository for immigration case data. CASE is covered by EOIR's Adjudication and Appeal Systems PIA available here: https://www.justice.gov/opcl/media/1347801/dl?inline.

practitioner; or (4) initiate formal disciplinary proceedings by filing a Notice of Intent to Discipline (NID) with the Board and serving a copy on the practitioner or recognized organization. Disciplinary hearings are generally conducted in the same manner as other EOIR immigration proceedings, as appropriate. The decision of an adjudicating official in a disciplinary proceeding may be appealed to the Board using the Form EOIR-45, Notice of Appeal from a Decision of an Adjudicating Official in a Practitioner Disciplinary Case.

In general, action taken on an NID may be disclosed to the public, and EOIR maintains on its public website a list of practitioners who have been disbarred, suspended, or publicly censured. This list is also posted for public awareness at immigration courts and the Board. Suspended or disbarred practitioners may seek reinstatement of their authorization to practice in immigration proceedings.

The AD Program uses an internal, web-based Microsoft Dynamics and SharePoint application for tracking, managing, and adjudicating disciplinary cases from initiation to completion. The AD System consists of two modules, one for AD Program staff and one for immigration judges and appellate immigration judges ("adjudicators"). The module for AD Program staff includes the following capabilities: record complaints received and initiate cases; automatically generate and assign case numbers; maintain an electronic case file to store all records relevant to a particular disciplinary case and any associated disciplinary proceeding; generate documents; query the CASE and eRegistry[2] systems to retrieve and link relevant immigration proceeding and practitioner data to disciplinary cases; and generate reports or display dashboards with metrics on case activity. The adjudicator module serves as the docketing and filing system for formal disciplinary proceedings. The adjudicator module includes the following capabilities: view and access filings in formal disciplinary proceedings; maintain an official electronic record of formal disciplinary proceedings; query the CASE system for relevant immigration proceeding information and documents; connect to the agency's digital audio recording system for purposes of recording disciplinary hearings; and issue notices, orders, and decisions in disciplinary proceedings.

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, 1158, 1229a, 1362.
Executive Order	
Federal regulation	8 C.F.R. §§ 1003.0(b), 1003.0(f), 1003.1(d)(2)(iii), 1003.1(d)(5), 1003.101-.111, 1292.1, 1292.3, 1292.19, 292.3.

[2] eRegistry is a public-facing, web-based applicabtion that enables legal practitioners seeking to represent individuals in EOIR immigration proceedings to register for an EOIR ID number, a number required before a practitioner can enter an appearance in a proceeding to serve as the practitioner of record in EOIR immigration proceedings. eRegistry is covered by EOIR's Adjudication and Appeal Systems PIA available here: https://www.justice.gov/opcl/media/1347801/dl?inline.

Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	Presidential Memorandum for the Attorney General and the Secretary of Homeland Security on Preventing Abuses of the Legal System and the Federal Courts (Mar. 21, 2025). EOIR PM 19-06, *Internal Reporting of Suspected Ineffective Assistance of Counsel and Professional Misconduct* (Dec. 18, 2018).

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.

(*continued next page*)

(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	Names of DOJ personnel, other Federal government personnel, and members of the public (USPER or non-USPER)
Date of birth or age	X	C, D	Date of birth or age of members of the public (USPER or non-USPER) may be included in complaints, EOIR practitioner registration records, or records of underlying immigration proceedings
Place of birth	X	C, D	Place of birth of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Sex	X	C, D	Sex of members of the public (USPER or non-USPER) may be included in complaints, EOIR practitioner registration records, or records of underlying immigration proceedings
Race, ethnicity, or citizenship	X	C, D	Race, ethnicity, or citizenship of members of the public (USPER or non-USPER) may be included in complaints, EOIR practitioner registration records, or records of underlying immigration proceedings
Religion	X	C, D	Religion of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	Full or partial social security numbers of members of the public (USPER or non-USPER) may be included in records of underlying immigration proceedings
Tax Identification Number (TIN)			
Driver's license	X	C, D	Driver's license information of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings

(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
Alien registration number	X	C, D	Alien registration number (A-number) of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Passport number	X	C, D	Passport numbers of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Mother's maiden name	X	C, D	Mother's maiden name of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Vehicle identifiers			
Personal mailing address, email address, and phone number	X	C, D	Personal mailing addresses of members of the public (USPER or non-USPER) may be included in complaints, EOIR practitioner registration records, or records of underlying immigration proceedings
Medical records number	X	C, D	Medical record numbers of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Medical notes or other medical or health information	X	C, D	Medical notes or other medical/health information of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Financial account information	X	C, D	Members of the public (USPER or non-USPER) may submit proof of payment of legal services as part of a complaint
Applicant information	X	C, D	Information contained in an application for recognition or accreditation, requests for an EOIRID number, or in notices of entry of appearance as practitioner of record in immigration proceedings submitted by members of the public (USEPR or non-USPER)
Education records	X	C, D	Education records or information of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings

(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
Military status or other information	X	C, D	Military status or information of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Employment status, history, or similar information	X	C, D	Employment status, history, or similar information of members of the public (USPER or non-USPER) who are subjects of disciplinary complaints or cases. This information may also be included in records of underlying immigration proceedings.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C, D	Private bar or professional licensing and disciplinary information of members of the public (USEPR or non-USPER) who are subjects of complaints or cases
Certificates			
Legal documents	X	C, D	Notices, orders, and decisions issued by EOIR adjudicators in disciplinary or immigration proceedings; photocopies of legal documents of members of the public (USPER or non-USPER) may be included in complaints, submitted by individuals who are subjects of complaints or cases, or included in records of underlying immigration proceedings
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C, D	Complainants may provide links to websites if relevant to the complaint
Foreign activities	X	C, D	Foreign activities of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	Criminal records information of members of the public (USPER or non-USPER) may be included in complaints, submitted by complaint or case subjects, or included in records of underlying immigration proceedings
Juvenile criminal records information	X	C, D	Juvenile criminal records information of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings

(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
Civil law enforcement information, e.g., allegations of civil law violations	X	C, D	Civil law enforcement information of members of the public (USPER or non-USPER) may be included in complaints, submitted by complaint or case subjects, or included in records of underlying immigration proceedings
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information	X	C, D	Grand jury information of members of the public (USPER or non-USPER) may be included in complaints, submitted by complaint or case subjects, or included in records of underlying immigration proceedings
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	Witness statements from members of the public (USPER or non-USPER) may be collected if relevant to the complaint or case
Procurement/contracting records			
Proprietary or business information	X	C, D	Business information of members of the public (USPER or non-USPER) may be included in complaints, submitted by complaint or case subjects, or collected during the course of an investigation
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C, D	Photos of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
- **Video containing biometric data**			
- **Fingerprints**	X	C, D	Photocopies of fingerprints of members of the public (USPER or non-USPER) are included in records of underlying immigration proceedings
- **Palm prints**			
- **Iris image**			
- **Dental profile**			

(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
- **Voice recording/signatures**	X	A, B, C, D	Digital audio recordings of formal disciplinary proceedings before an Adjudicating Official or the Board capture voice recordings
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**	X	C, D	Physical descriptors of members of the public (USPER or non-USPER) may be included in complaints or in records of underlying immigration proceedings
System admin/audit data:			
- **User ID**	X	A	User ID of authorized EOIR users
- **User passwords/codes**	X	A	Passwords of authorized EOIR users
- **IP address**	X	A	IP address of authorized EOIR users
- **Date/time of access**	X	A	Date/time of access of authorized EOIR users
- **Queries run**	X	A	User activity and audit logs of authorized EOIR users
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Disciplinary or fraud complaint and case numbers linkable to members of the public (USEPR or non-USPER) submitting complaints, who are subjects of complaints or cases, or who are witnesses in cases. State bar or professional license numbers and EOIRID numbers of members of the public (USPER or non-USPER) who are subjects of complaints or cases. EOIR anticipates that the AD System will primarily handle the above categories of information, but it is possible that complainants, subjects of complaints or cases, and witnesses may voluntarily provide additional categories of information believed to be relevant to the complaint or case.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax	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): Anyone may submit complaints, including individuals within government entities.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Anyone may submit complaints, including individuals from the private sector.					

<u>Section 4</u>: 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	EOIR adjudicators have direct log-in access to a dedicated module in the AD System for purposes of adjudicating formal disciplinary proceedings.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X			Complaints regarding the conduct or behavior of Department attorneys, immigration judges, or appellate immigration judges are directed to the DOJ Office of Professional Responsibility. EOIR also shares information with the DOJ Executive Office of the United States Attorneys for civil or criminal investigation or prosecution of conduct that is the subject of AD complaints or cases. EOIR may also refer matters to the Inspector General or the Federal Bureau of Investigation, if appropriate.
Federal entities	X			EOIR shares information with the Department of Homeland Security (DHS), including the Disciplinary Counsel(s) for the U.S. Citizenship and Immigration Services, Homeland Security Investigations (HSI), and the Fraud Detection and National Security Directorate for investigation, law enforcement, or prosecution of conduct that is the subject of AD complaints or cases.
State, local, tribal gov't entities	X			EOIR shares information with state, local, or tribal government entities, including disciplinary or regulatory licensing authorities, for investigation, disciplinary or regulatory action, civil or criminal law enforcement, or prosecution of conduct that is the subject of AD complaints or cases.

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			The list of current and previously disciplined practitioners is made publicly available on EOIR's website and posted at the Board and immigration courts for public awareness, including copies of disciplinary orders. Complainants may receive limited access to specific case information related to their own complaints. Members of the public may also access information by submitting a Freedom of Information Act (FOIA) or Privacy Act (PA) request, subject to applicable exemptions.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Counsel, parties, and witnesses to AD complaints or cases may be provided with access to specific complaint or case information. Courts or judicial tribunals may access specific complaint or case information by court order or in the course of litigation if deemed relevant to the judicial proceeding.
Private sector	X			Private sector individuals or entities who are complainants may access specific complaint or case information. All others may receive access by submitting a FOIA request, subject to applicable exemptions.
Foreign governments	X			Foreign governments may obtain complaint or case information by submitting a FOIA request, subject to applicable exemptions.

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 entities	X			Foreign entities may obtain complaint or case information by submitting a FOIA request, subject to applicable exemptions.
Other (specify):	X			EOIR transmits notices of all public discipline imposed under 8 C.F.R. §§ 1003.101-.111 to the National Lawyer Regulatory Data Bank maintained by the American Bar Association. Members of the public or other entities may obtain information from EOIR by submitting a FOIA or PA request, subject to applicable exemptions, or by producing written consent from a records subject to access the information.

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.

Information related to currently or previously disciplined practitioners is available on data.gov located here https://catalog.data.gov/dataset/attorney-discipline. The information disclosed is limited to the disciplined practitioner's name, location (city/state) of licensure or practice, type of discipline imposed, dates/duration of discipline, and reinstatement date (if any). Copies of disciplinary orders are publicly available as a measure to warn or protect the public from harm from disciplined practitioners. When practitioners enter their appearance on the record in EOIR immigration proceedings using Forms EOIR-27 (OMB No. 1125-0005) or EOIR-28 (OMB No. 1125-0006), the practitioner explicitly consents to EOIR publishing his or her name and any findings of misconduct should the individual become subject to any public discipline by EOIR pursuant to the rules and procedures at 8 C.F.R. § 1003.101 *et seq*.

<u>Section 5:</u> 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 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 and available for convenience on the DOJ website (https://www.justice.gov/opcl/doj-systems-records#EOIR); (2) Privacy Act Statements, pursuant to 5 U.S.C. § 552a(e)(3), displayed on EOIR information collections and applications that collect PII; and (3) the DOJ Privacy Policy, available 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.

Most information collected by the system is provided voluntarily by individuals, and individuals may decline to provide information to the agency. EOIR notifies individuals that failure to provide certain information may impact the processing of their complaint or their eligibility to serve as a legal representative before EOIR. Under 8 C.F.R. § 1003.103(c), practitioners are obligated to self-report certain information impacting their ability to practice law, and the failure to self-report this information may result in an immediate suspension and other final disciplinary action imposed by EOIR.

Generally, information concerning attorney discipline complaints or preliminary inquiries is confidential, though there are required or permissible exceptions by law or regulation, as described at 8 C.F.R. § 1003.108. Generally, individuals may waive such confidentiality restrictions, subject to applicable exemptions under law or regulation. For attorney discipline complaints specifically, a complainant explicitly waives attorney-client privilege or other confidentiality protections so that the Disciplinary Counsel may disclose information as necessary to complete an investigation. When practitioners enter their appearance on the record in EOIR immigration proceedings using Forms EOIR-27 (OMB No. 1125-0005) or EOIR-28 (OMB No. 1125-0006), the practitioner explicitly consents to EOIR publishing his or her name and any findings of misconduct should the individual become subject to any public discipline by EOIR pursuant to the rules and procedures at 8 C.F.R. § 1003.101 *et seq*. Individuals may also consent to release information about themselves to designated recipients using the Form EOIR-59, Certification and Release of Records (OMB No. 1125-0017).

Individuals generally do not have the ability to consent to specific uses of their information pursuant to applicable SORNs. Individuals also do not have the ability to consent to the disclosures required or otherwise committed to the Disciplinary Counsel's discretion by the regulations governing the AD Program, including but not limited to disclosures to DHS, law enforcement authorities, and appropriate Federal or state disciplinary or regulatory authorities. *See* 8 C.F.R. §§ 1003.101-.111.

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 AD System in the following ways: (1) individuals may submit a FOIA request for a copy of certain case information related to those complaints; or (2) individuals may submit a Privacy Act request with EOIR's FOIA Office. Individuals may submit a Privacy Act request to amend or correct PII maintained by the agency. Instructions for making FOIA and Privacy Act requests are available on the EOIR website (https://www.justice.gov/eoir/freedom-information-act-foia).

The Attorney General has exempted certain records in the AD System from the access provisions of the Privacy Act, pursuant to 5 U.S.C. § 552a(k)(1) and (k)(2), because they contain investigatory material compiled for law enforcement purposes, as stated in Order No. 18-86, 51 FR 32305 (Sept. 11, 1986), as amended by Order No. 180-99, 64 FR 61787 (Nov. 15, 1999). *See* 28 C.F.R. § 16.83. Nonetheless, EOIR takes seriously its obligation to maintain accurate records and, in its sole discretion, agrees to permit amendment or correction of EOIR records and will share that information in appropriate cases with subjects of the records.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** The AD system is within the JCON/eWorld Adjudication Support ATO, granted August 29, 2025, and expiring August 29, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs)**

	for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: Currently, 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:
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:** The system is categorized as Moderate based upon the particular information types handled by the system. The system handles information pertaining to administrative adjudications, administrative investigations, and in some instances, criminal proceedings. A loss of confidentiality, availability, and/or integrity of such information could be expected to have a serious adverse effect on EOIR operations or assets or individuals.
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 alerts 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:** Audit logs are collected and maintained for 120 days and are reviewed weekly by EOIR's Office of Information Technology 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:** New staff members for the AD Program undergo system-specific training during orientation and onboarding. System user manuals and guides are also available to system users.

6.2 Explain key privacy and security administrative, technical, or physical controls that are

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

Access to the AD System is limited to authorized EOIR employees and contractors responsible for administering the program or as system administrators. User permissions and access to information in each system are tailored based on the particular user's role. To maintain access to the system, EOIR users are required to annually complete cybersecurity and privacy awareness trainings and to review and sign the DOJ Cybersecurity and Privacy Rules of Behavior. Users are also provided with system-specific training. Authorized users may only access the system after verifying their identity with multi-factor authentication. EOIR user accounts are reviewed annually to determine whether continued access is necessary, and users accounts are automatically disabled after 90 days of inactivity. User accounts are locked for specified periods of time after a specified number of unsuccessful log-in attempts.

System user activity is regularly monitored, logged, and audited to detect suspicious activity. EOIR also conducts regular vulnerability scanning and configuration management activities to minimize privacy and security risks associated with the download of any content submitted by email to the AD Program and subsequently entered into the system.

Systems are only available internally on EOIR's private network. Information is encrypted in transit and at rest. EOIR also utilizes a variety of other security mechanisms to minimize privacy and security risks, including but not limited to firewalls and antivirus software.

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.

AD Program records are retained and disposed of in accordance with National Archives and Records Administration (NARA) schedule DAA-0582-2017-0002. Retention periods vary based on the type of disciplinary case and range from 2 to 25 years. Formal Discipline Case Files are temporary records with a retention period of 15 years after cutoff (DAA-0582-2017-0002-0001 and DAA-0582-2017-0002-0005). Non-Reinstatement Case Files are temporary records with a retention period of 25 years after cutoff or when the death of the subject occurs, whichever is sooner (DAA-0582-2017-0002-0002). Referral, Warning, and Admonition Case Files are temporary records with a retention period of 6 years after cutoff (DAA-0582-2017-0002-0003). Case Files Closed Without Further Action on a Complaint are temporary records with a retention period of 2 years after cutoff (DAA-0582-2017-0002-0004). Requests for Reinstatement Case Files are temporary records with a retention period of 10 years after cutoff (DAA-0582-2017-0002-0006).

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, Adjudication and Appeal Records of the Office of the Chief Immigration Judge and Board of Immigration Appeals, 90 FR 42265 (Aug. 29, 2025), https://www.justice.gov/opcl/media/1421316/dl?inline.

- 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/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? 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.***

The AD complaint submission methods create opportunities for EOIR to collect more information than may be necessary to administer the program. Specifically, there are opportunities for individuals to voluntarily provide information that the agency did not request or does not require to process, investigate, and/or adjudicate complaints. Pursuant to its obligations under the Paperwork Reduction Act, EOIR regularly reviews its information collections to ensure it only solicits the minimum amount of information necessary and relevant to the AD Program. Additionally, EOIR provides guidance to individuals on its agency forms and electronic information collection instruments to advise the individual on the scope of information that the agency requires.

The system maintains large quantities of PII, and EOIR must exert significant efforts to ensure the PII is accurate and reliable. For this reason, information in the systems is organized and clearly labeled by case type (Complaint, Case, Closed Case, etc.) and tracked using unique numerical identifiers. To ensure record contents are accurate and reliable, EOIR primarily relies on individuals to contact the agency to update its records and maintain the integrity of EOIR's records. EOIR provides individuals with several methods by which the individual can update agency records about the individual, including those described in Section 5.3 above.

EOIR must ensure that PII is not maintained longer than necessary because prolonged retention increases the risk of PII spills. Records and data are promptly removed from the system upon specific sunset deadlines when a record reaches its cutoff period and then disposed of in accordance with applicable record retention schedules.

EOIR manages high volumes of records requests, which requires the agency to obtain consent to disclose information, to verify authority to disclose information absent consent, and to only disclose the minimum amount of information necessary to respond to the particular request. EOIR has streamlined its processes to obtain consent from individuals to disclose their records by making available Form EOIR-59. EOIR directs all requests for information to OGC for review pursuant to laws and regulations governing information sharing and disclosure, such as FOIA, the Privacy Act (including applicable SORNs), the Immigration and Nationality Act (INA), 8 U.S.C. § 1367, and 8 C.F.R. § 1208.6. When fulfilling requests for statistical data or publishing statistical data to its website, EOIR deidentifies data by anonymizing and/or aggregating data.

Some information received by the AD Program is often confidential or subject to attorney-client or other privileges that would ordinarily prohibit the agency from sharing such information. EOIR clearly advises on the Form EOIR-44 and other program materials that by submitting a complaint, the individual waives any attorney-client privilege or other confidentiality/privacy protection with respect to the practitioner's or organization's handling of an immigration case to the extent necessary for the Disciplinary Counsel to conduct an inquiry. EOIR also advises that it may disclose information and records to state bar or law enforcement authorities where it appears the practitioner or organization has engaged in ethical and/or criminal misconduct. When EOIR does disclose information and records to such authorities, EOIR redacts the irrelevant PII of third parties identified in the records.

Given the volume, nature, and sensitivity of information handled by the system, EOIR must carefully monitor access to and use of the information to prevent unauthorized access, use, disclosure, or destruction of information. EOIR mitigates these risks by only granting internal access to employees or contractors who complete the requisite background check process, identity validation, and annual security and privacy training, and who annually review and acknowledge DOJ's Cybersecurity and Privacy Rules of Behavior to maintain system access. System access, data storage, and capabilities to create, modify, or delete data files are all restricted based on user roles and permissions. User accounts are reviewed regularly and deactivated after a specified period of inactivity. User activity audits are conducted regularly to monitor suspicious activity. Several security measures are in place to safeguard information in the systems, including 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 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, contracts provisions are in place to manage and control access to EOIR information by its contractors. Contracts with vendors contain security language required by the DOJ, including contracts for FedRAMP-authorized cloud services, such as the Microsoft Azure Cloud supporting critical infrastructure for the AD System. Contracts also 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.