Executive Office for Immigration Review

Privacy Impact Assessment
for the
Fraud and Abuse Prevention Program

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)

Section 1: Executive Summary

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

The Executive Office for Immigration Review's (EOIR) primary mission 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.

Within EOIR's Office of the General Counsel (OGC), under the supervision of a designated anti-fraud officer, the Fraud and Abuse Prevention Program (Fraud Program) receives, processes, tracks, manages, investigates, and responds to complaints of immigration fraud, immigration scams, and the unauthorized practice of immigration law within EOIR immigration proceedings. When appropriate, the Fraud Program refers complaints to law enforcement and disciplinary authorities for further action, investigation, or prosecution. The Fraud Program collects, maintains, and disseminates personally identifiable information (PII) of complainants, witnesses, and subjects of complaints in order to respond to suspected immigration fraud reported to the Program, including but not limited to complainant and witness names and contact information, physical descriptors, alien registration numbers (A-numbers), EOIR ID numbers, and personal information submitted in evidentiary records submitted to or collected by the Program during the course of an investigation. Such information is maintained in a system of case files and reports generated and maintained by the Fraud Program.

EOIR initially included the Fraud Program in the 2018 Privacy Impact Assessment (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 technologies supporting the Fraud Program have undergone significant changes: new types of information were added to the systems; some on-premises components of the systems were migrated to cloud-based components; and the electronic Microsoft Dynamics system previously serving as the Program's case management system has been decommissioned. Such changes present new privacy risks or concerns, 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.

The Fraud Program, led by a designated anti-fraud officer, serves as the agency's point of contact relating to concerns about possible immigration fraud perpetrated in the context of EOIR immigration proceedings. 8 C.F.R. § 1003.0(f)(2). The Fraud Program investigates complaints of immigration fraud, scams, and unauthorized practice of immigration law; refers complaints of fraud to appropriate federal, state, local, territorial, or tribal law enforcement and disciplinary authorities; supports investigations, prosecutions, and disciplinary proceedings conducted by such authorities; trains EOIR personnel on identifying immigration fraud; and publicly disseminates informative and educational resources on immigration fraud issues. When a complaint involves an attorney or accredited representative, the Fraud Program may refer the matter to EOIR's Attorney Discipline (AD) Program to investigate whether the practitioner engaged in criminal, unethical, or unprofessional conduct in violation of 8 C.F.R. §§ 1003.101-.111.

Fraud complaints are typically submitted to the Program by email and include a description of the suspected fraud and the people involved, including names, dates, addresses, and other identifying information the complainant determines to be relevant. Complaints may be submitted by members of the public, DOJ personnel, or personnel from other Federal agencies. Complaints involving EOIR immigration proceedings are elevated to a "case" status with the Fraud Program; complaints that do not involve EOIR immigration proceedings are reported to the appropriate authority for investigation. The Fraud Program investigates a case until it is determined to be unsubstantiated or until some discipline, sanction, or prosecution has completed the process. The Fraud Program assigns unique numbers to each complaint and case and compiles an evidentiary file for each complaint and case. Evidentiary files include complaints, witness statements, correspondence, notes, and any other information or documents provided by complainants or collected by Program staff during the course of an investigation. Program staff may correspond with complainants or other witnesses to gather additional information as needed to substantiate complaints. All information provided to the Fraud Program is voluntarily provided by complainants and witnesses or otherwise gathered from publicly available information on the internet. Program staff may also copy or collect relevant information from the official records of any underlying immigration proceedings impacted by the alleged fraud. Official records of immigration proceedings are accessed by authorized Fraud Program staff using the Case Access System for EOIR (CASE)[1] or the EOIR Courts and Appeals System (ECAS).[2] The Fraud

---

[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.

[2] ECAS is a suite of internal and public-facing, web-based applications to manage electronic documents in immigration proceedings before EOIR's immigration courts and the Board, from initial submission of electronic documents by the parties to maintenance and storage of the official electronic record of immigration proceedings to

Program closes a case upon determination that it will not be pursuing the matter further and/or has notified appropriate law enforcement or disciplinary authorities of substantiated matters.

The Fraud Program collects, maintains, and disseminates personally identifiable information (PII) of complainants, witnesses, and subjects of complaints in order to respond to suspected immigration fraud reported to the Program. This PII includes: complaints or case numbers, status, and dates; names and contact information of complainants, witnesses, subjects, and law enforcement or disciplinary authorities; date of birth, age, sex, physical descriptors, alien registration numbers (A-numbers), and/or EOIR ID numbers of complainants, witnesses, or subjects; and personal information within evidentiary records submitted with complaints or obtained in the course of substantiating complaints of alleged fraud. Such information is maintained in a system of case files and reports generated and maintained by the Fraud Program.

Fraud Program complaint and case files were previously logged, tracked, and managed from receipt through closure using a web-based Microsoft Dynamics application. This application was decommissioned in 2025, and the records were either transferred to existing agency network drives or disposed of in accordance with applicable records retention schedules. Currently, the Fraud Program utilizes the Microsoft Office 365 suite and a shared internal network drive hosted on the EOIR Microsoft Azure Cloud to create, maintain, and store fraud complaints and case files. The Fraud Program records maintained by EOIR consist primarily of electronic records.[3]

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. §§ 1101, 1103, 1154, 1158-59, 1229a, 1255, 1255a, 1324a, 1324b, 1324c, 1362.
Executive Order	
Federal regulation	8 C.F.R. parts 1001 and 1003; 8 C.F.R. §§ 1003.0, 1003.1(d)(2)(iii), 1003.1(d)(5), 1003.101-.111, 1292.1, 1292.3, 1292.19, 292.3; 28 C.F.R. §§ 68.33, 68.35-.36.
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 Court (Mar. 22, 2025); EOIR Policy Memorandum (PM) 25-19 (Amended), *EOIR's Anti-*

use of electronic documents by agency adjudicators in issuing notices and orders. ECAS is covered by EOIR's Adjudication and Appeal Systems PIA available here: https://www.justice.gov/opcl/media/1347801/dl?inline.

[3] Though some complaints may be submitted by mail, such records are converted to electronic records. Records received in hard copy are digitized and then disposed of following quality control checks of the digital copies, in accordance with authorized agency records information management practices.

	Fraud Program (Feb. 5, 2025); EOIR PM 19-07, *Identifying and Reporting Fraud and Abuse* (Dec. 19, 2018); 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.

(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 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 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 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
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
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 address, email address, and phone number of members of the public (USPER or non-USPER) may be included in complaints or records of underlying immigration proceedings
Medical records number	X	C, D	Medical records number 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

(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
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 EOIR ID 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
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 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			

(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
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
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

(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
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 are included in records of underlying immigration proceedings
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, D	Digital audio recordings of EOIR immigration or disciplinary proceedings 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 EOIR users
- **User passwords/codes**	X	A	Passwords of EOIR users
- **IP address**	X	A	IP address of EOIR users
- **Date/time of access**	X	A	Date/time of access of EOIR users
- **Queries run**	X	A	User activity and audit logs of EOIR users
- **Contents of files**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	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 EOIR ID numbers of members of the public (USPER or non-USPER) submitting complaints, who are subjects of complaints or cases, or who are witnesses in cases. EOIR anticipates the Fraud Program 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. Phone numbers and addresses of notarios[4] suspected of engaging in fraud or the unauthorized practice of law are collected through public websites advertising alleged fraudulent immigration services.					

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			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 Office of the United States Attorneys for civil or criminal investigation or prosecution of conduct that is the subject of fraud complaints or cases. EOIR may also refer matters to the Inspector General or the Federal Bureau of Investigation, if appropriate.

[4] Notarios are generally individuals who hold themselves out as qualified to provide legal advice concerning immigration though such individuals in fact have no such qualifications.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X			EOIR shares information with the Federal Trade Commission and 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 fraud complaints or cases
State, local, tribal gov't entities	X			EOIR shares information with state, local, or tribal government entities, including law enforcement or disciplinary authorities, for investigation, disciplinary or regulatory action, civil or criminal law enforcement, or prosecution of conduct that is the subject of fraud 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 Fraud Program makes Scam Alerts publicly available on its website to raise public awareness of fraud issues, though Scam Alerts only include the general, de-identified details received about substantiated complaints. 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 fraud 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 or PA 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):				

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.

Fraud Program information is not released to the public for "Open Data" purposes. However, the Fraud Program posts general Scam Alerts on the EOIR website at https://www.justice.gov/eoir/fraud-and-abuse-prevention-program. Scam Alerts are general, de-identified descriptions of substantiated fraud reported to the Program to raise public awareness about immigration fraud scams. EOIR does not include identifying information from complaints in the Scam Alerts.

Section 5: Notice, Consent, Access, and Amendment

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

EOIR 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 public-facing 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.

Individuals are not required to submit complaints. Most information collected by the Fraud Program 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. Generally, individuals do not have an opportunity to consent to disclosures of their information to investigative and law enforcement authorities because EOIR is required to coordinate with such agencies to identify and respond to reported fraud. 8 C.F.R. § 1003.0(f)(2)(ii)-(iii).

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 maintained by the Fraud Program by submitting a FOIA or Privacy Act request to EOIR's Office of the General Counsel. Privacy Act requests may also be submitted to amend or correct PII maintained by EOIR. Instructions for making FOIA and Privacy Act requests are available on the EOIR website (https://www.justice.gov/eoir/freedom-information-act-foia).

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 Fraud Program 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 information is this 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 continuous monitoring of cybersecurity incidents and alerts and conducts annual testing of the incident response plan.
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 Fraud Programs undergo program-specific training during orientation and onboarding.

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 Fraud Program records is limited to authorized EOIR employees and contractors responsible for administering the program or with an authorized need to know the information to perform their job duties. User permissions and access to information on the designated shared network drive are tailored based on the particular user's role. Generally, to maintain access to the shared drive, 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. Authorized users may only access the shared drive after logging into their DOJ device and 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 Fraud Program and subsequently ingested into EOIR systems.

The shared drive is 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.

Fraud Program records are retained and disposed of in accordance with National Archives and Records Administration (NARA)-approved schedule DAA-0582-2017-0001. The Immigration Fraud and Abuse Prevention Program case files and data are temporary records retained for 15 years after cutoff (DAA-0582-2017-0001-0001 and DAA-0582-2017-0001-0002). The Fraud and Abuse Prevention Program newsletters are temporary records disposed of five (5) years after cutoff (DAA-0582-2017-0001-0003). The Fraud and Abuse Prevention working files are temporary records with a retention period of three (3) years after cutoff (DAA-0582-2017-0001-0004). Fraud Program Items Closed without Action are temporary records retained for three (3) years after cutoff (DAA-0582-2017-0001-0005). To the extent that any records maintained by the Fraud Program are not scheduled, any unscheduled records will be retained until they are scheduled.

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:

EOIR is in the process of developing a SORN specifically for Fraud and Abuse Prevention Program Records. Some Fraud Program records are currently covered in part by the following published SORNs:

- 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 fraud complaint submission method creates 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, or refer complaints to law enforcement authorities. To minimize the collection of unnecessary information, EOIR attempts to provide guidance to complainants and witnesses on the scope of information that the agency requires to substantiate or refer complaints. Fraud Program staff are trained to not include irrelevant information in fraud case files to the extent possible.

The Fraud Program maintains large quantities of PII, and EOIR must exert significant efforts to ensure the PII is accurate and reliable to the extent possible. For this reason, information in the systems is organized and clearly labeled by complaint or 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. This risk is minimized as the Fraud Program promptly disposes of its records and data in accordance with applicable records retention schedules.

While EOIR generally manages high volumes of records requests, very few record requests received by EOIR are for Fraud Program records. For all record requests, EOIR should consistently implement measures 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, Certification and Release of Records (OMB Control No. 1125-0017). 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.

Generally, individuals do not have an opportunity to consent to disclosures of their information to investigative and law enforcement authorities because EOIR is required to coordinate with such agencies to identify and respond to reported fraud. 8 C.F.R. § 1003.0(f)(2)(ii)-(iii). EOIR has provided notice to the public about this and other routine uses of its information through the SORNs identified in Section 7.2 of this PIA.

Given the volume, nature, and sensitivity of information handled by the Fraud Program, EOIR must carefully monitor access 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 or edit 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 (FTP), 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 technological infrastructure for the Fraud Program. 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.