This document is scheduled to be published in the Federal Register on 2026-10-15 and available online at https://www.federalregister.gov/d/2026-21062, and on https://govinfo.gov

e: 4410-30-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 013-2026]

Privacy Act of 1974; Systems of Records

AGENCY: Executive Office for Immigration Review, United States Department of Justice.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Executive Office for Immigration Review (EOIR), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records notice titled "Fraud and Abuse Prevention Program Records," and numbered JUSTICE/EOIR-006. This system of records assists the EOIR Fraud and Abuse Prevention Program (Fraud Program) in receiving, tracking, and managing complaints of suspected immigration fraud, abuse, and unauthorized practice of immigration law, and in referring complaints to Federal, state, and local law enforcement and disciplinary authorities when appropriate. Fraud Program records were previously included within a different system of records, JUSTICE/EOIR-001. *See* 69 FR 16179 (May 11, 2004). However, JUSTICE/EOIR-001 was recently modified and now only partially covers Fraud Program records. *See* 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). Accordingly, EOIR proposes to establish a new system of records encompassing all Fraud Program records.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Routine uses will become effective after the 30-day comment period.

Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The public, OMB, and Congress are invited to submit any comments by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, Two Constitution Square (2CON), 145 N Street, NE, Suite 8W.300, Washington, DC 20530; by facsimile at 202-307-0693; or by email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Justine Fuga, Senior Component Official for Privacy, Office of the General Counsel; Executive Office for Immigration Review, 5107 Leesburg Pike, Suite 2600, Falls Church, VA 22041; Justine.Fuga@usdoj.gov; EOIR.Privacy.Intake@usdoj.gov.

SUPPLEMENTARY INFORMATION:

The primary mission of 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.

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) investigates complaints of immigration fraud, immigration scams, and the unauthorized practice of immigration law within EOIR proceedings. The Fraud Program refers complaints of fraud to appropriate law enforcement and disciplinary authorities; and it provides training for EOIR personnel, outreach materials, and education for the public on these issues. *See* 8 C.F.R. 1003.0(f)(2).

The anti-fraud officer serves as a point of contact relating to concerns about possible fraud involving EOIR proceedings, particularly with respect to matters relating to fraudulent applications or documents affecting multiple removal proceedings, applications for relief from removal, appeals, or other proceedings before EOIR. 8 C.F.R. 1003.0(f)(2)(i). The Fraud Program coordinates with investigative authorities of the Department of Justice, Department of Homeland Security, and other appropriate agencies with respect to the identification of and response to reported fraud. 8 C.F.R. 1003.0(f)(2)(ii). The Fraud Program also collaborates with the EOIR disciplinary counsel and with other appropriate authorities with respect to instances of fraud, misrepresentation, or abuse pertaining to an attorney or accredited representative providing representation to clients in EOIR immigration proceedings. 8 C.F.R. 1003.0(f)(2)(iii).

This system of records is used by the Fraud Program in connection with its work receiving, tracking, managing, investigating, and responding to reports of suspected immigration fraud, abuse, and unauthorized practice of immigration law, and referring complaints to Federal, state, local, territorial, or tribal law enforcement and disciplinary authorities when appropriate. The system consists primarily of electronic records. Records received in hard copy are digitized and the hard copies are disposed of following quality control checks of the digital copies, in accordance with authorized agency records information management practices. Records are stored on the DOJ EOIR Microsoft Azure Cloud in agency shared drives and disposed of in accordance with applicable record retention schedules. As such, EOIR has prepared this system of records notice to account for the changes to JUSTICE/EOIR-001, resulting in the need for a system of records specific to the Fraud Program system of records.

Finally, pursuant to 5 U.S.C. 552a(k)(2), EOIR claims that information in this system is exempt from 5 U.S.C. 552a(c) and (d). Rules will be promulgated in

accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and will be published and codified in the Federal Register at 28 CFR 16.83.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new system of records.

Dated: October 5, 2026.

Laurence E. Rothenberg,

Chief Privacy and Civil Liberties Officer,

United States Department of Justice.

JUSTICE/EOIR-006

SYSTEM NAME AND NUMBER:

Fraud and Abuse Prevention Program Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Executive Office for Immigration Review, Department of Justice, 5107 Leesburg Pike, Suite 2600, Falls Church, Virginia 22041. Electronic records are maintained and stored in network drives hosted on the DOJ EOIR Microsoft Azure Cloud.

SYSTEM MANAGER(S):

General Counsel, Office of the General Counsel, Executive Office for Immigration Review, 5107 Leesburg Pike, Suite 2600, Falls Church, VA 22041.

Chief Information Officer, Office of Information Technology, Executive Office for Immigration Review, 4825 Mark Center Drive, Suite 200, Alexandria, VA 22311.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. 1101, 1103, 1154, 1158-59, 1229a, 1255, 1255a, 1324a, 1324b, 1324c, 1362; 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, 68.36; 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-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).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to maintain records of the Fraud Program in connection with its work receiving, tracking, managing, investigating, and responding to reports of suspected immigration fraud, abuse, and unauthorized practice of immigration law, and referring complaints to law enforcement and disciplinary authorities when appropriate. The records in the system are also used to generate statistical reports, informational materials for public awareness concerning immigration fraud issues, and internal materials to train EOIR personnel in identifying and reporting suspected fraud.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system includes records pertaining to complainants, witnesses, and subjects of investigations of alleged fraud; EOIR adjudicators and personnel reporting, observing, or investigating alleged fraud; individuals who are subjects of EOIR immigration proceedings; attorneys, representatives, and organizations practicing before EOIR adjudicators; and law enforcement and disciplinary authorities to which the Fraud Program refers complaints.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes the following categories of electronic records: Fraud Program case files, related data, and education and training materials.

Fraud Program case files consist of: complaints of fraud, including the complainant's contact information; evidentiary records submitted with complaints or collected during the course of investigating and substantiating complaints, including copies of relevant portions of official records of immigration proceedings and digital audio recordings of immigration hearings; correspondence, witnesses statements, memoranda, and notes collected or created in the course of investigating and substantiating complaints; correspondence with law enforcement and disciplinary authorities to which a complaint may be referred.

Fraud Program data contained in the records in this system consists of: complaints, including case number and status; the date a complaint or case was reported or closed; names and contact information of complainants, witnesses, subjects, and law enforcement or disciplinary authorities; and date of birth, age, sex, and physical descriptors of the complainants, witnesses, or subjects, as well as their alien registration number (A-number), and/or EOIR ID numbers. Fraud Program data is used to generate statistical reports.

This system includes general educational materials, including the Fraud Program Newsletter, created by the Fraud Program for purposes of informing and raising internal and/or public awareness concerning immigration-related fraud issues. The system also includes internal training materials and presentations developed by the Fraud Program to train EOIR personnel on identifying and reporting suspected fraud.

RECORD SOURCE CATEGORIES:

Records in this system are generated or provided by members of the public; EOIR personnel; and law enforcement or disciplinary authorities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), all or a portion of the records contained in this system of records may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information in the record was collected:

1) To the Department of Homeland Security (DHS), including but not limited to the Disciplinary Counsel(s) for the U.S. Citizenship and Immigration Services (USCIS), Homeland Security Investigations, and Fraud Detection and National Security Directorate, to investigate and respond to complaints of fraud;

2) To Federal agencies, including but not limited to the Federal Trade Commission and DHS, involved in statistical analysis of data, and publication and/or reporting of aggregated or de-identified information designed to improve the efficiency and effectiveness of immigration proceedings at those agencies or to better meet EOIR's mission of adjudicating cases fairly, expeditiously, and uniformly interpreting and administering the Nation's immigration laws.

3) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature –to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

4) To any person or entity that EOIR has reason to believe possesses information regarding a matter within the jurisdiction of EOIR, to the extent deemed to be necessary by EOIR in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity, such as to assist EOIR in evaluating and substantiating claims of immigration-related fraud or abuse or unauthorized practice of immigration law.

5) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department or an adjudicator determines that the records are relevant to the proceeding; or when the records are relevant to a proceeding and the DOJ or any subcomponent thereof is authorized to appear in it; or when any of the following is a party to litigation or has an interest in litigation: DOJ or any components thereof; any DOJ employee in his or her official capacity; any DOJ employee in his or her individual capacity where DOJ has agreed to represent the employee; or the United States where DOJ or any

component thereof determines that litigation is likely to affect it or any of its subdivisions.

6) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or in connection with settlement, plea bargaining, or discovery proceedings, whether formal or informal.
7) To the news media and the public, including disclosures pursuant to 28 C.F.R. 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the agency, when necessary to accomplish an agency function related to this system of records.
9) To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is necessary to the recipient agency's decision.
10) To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

11) To a former employee of the Department for purposes of responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority; in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

12) To Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

13) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

14) To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

15) To appropriate agencies, entities, and persons when (i) the Department suspects or has confirmed that there has been a breach of the system of records; (ii) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (iii) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

16) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the

recipient agency or entity in (i) responding to a suspected or confirmed breach, or (ii) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

17) To any Federal Office of the Inspector General, or similar publicly identified official of a federal agency who has the official mission and duty to detect and deter waste (the squandering of money or resources even if not explicitly illegal), fraud (the attempt to obtain something of value through willful misrepresentation), and abuse (behaving improperly or unreasonably, or misusing one's position or authority), as necessary for the purpose of identification and elimination of such waste, fraud, and abuse related to Federal programs, employees, contractors, grantees, inmates, or beneficiaries.

18) To such recipients and under such circumstances and procedures as are mandated by federal statute, regulation, or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

All electronic records in this system are stored in electronic media via a configuration of government servers and in accordance with Federal and Department information security standards. Records received in hard copy are digitized. Digitized copies undergo quality control checks to confirm the digitization of the records was complete and accurate before the original hard copy is disposed of in accordance with authorized agency record information management practices. Records in this system are maintained in accordance with applicable laws, rules, and policies on protecting individual privacy and operating in a Federal Risk and Authorization Management Program (FedRAMP) certified cloud-storage environment. Stored records are organized

by complainant name, complaint or case number, complaint or case type and date, complaint or case status, and/or the name of the subject of the complaint or case.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by complainant name, complaint or case type, complaint or case numbers, date the complaint or case was reported or closed, and/or the name of the subject of the complaint or case. Records may only be retrieved by authorized DOJ personnel on a need-to-know basis.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained in accordance with EOIR Agency Records Control 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 5 years after cutoff (DAA-0582-2017-0001-0003). The Fraud and Abuse Prevention Working Files are temporary records with a retention period of 3 years after cutoff (DAA-0582-2017-0001-0004). Fraud Program Items Closed without Action are temporary records retained for 3 years after cutoff (DAA-0582-2017-0001-0005).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable laws, rules, and policies that protect individual privacy, including automated system security and access policies of EOIR and the Department. Access to records is limited to Department personnel who have an official need for access in order to perform their duties. Electronic records are maintained and backed up on secure servers and networks that may only be accessed by authorized personnel. Physical records are stored in locked filing cabinets or locked offices until they are digitized and disposed of, as described above. Access to

records may be restricted depending on a user's role and responsibility within the system. Internet connections are protected by multiple firewalls. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance, and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations. Users of individual computers can only gain access to the data by authorized user identification and authentication processes. Records are safeguarded in accordance with appropriate laws, rules, and policies based on the classification and handling restrictions of the record.

RECORD ACCESS PROCEDURES:

All requests for access to records must be made in writing and include a general description of the records sought and identifying information about the record subject, including but not limited to, the record subject's full name, date of birth, place of birth, and alien registration number (A-number), where applicable. *See* 28 C.F.R. 16.41; 28 C.F.R. part 16 Appendix I. If the A-number is not known, or the case occurred before 1988, the date of an Order to Show Cause, country of origin, and location of the immigration hearing must be provided. *See* 28 CFR part 16 Appendix I.

All requests for access to records may be submitted by mail to EOIR's Freedom of Information Act (FOIA) Service Center at 5107 Leesburg Pike, Suite 2600, Falls Church, VA 22041, by email at EOIR.FOIARequests@usdoj.gov, or online through the EOIR FOIA Public Access Link, available at https://foia.eoir.justice.gov/app/Home.aspx. Additional information for submitting requests to the FOIA Service Center can be found at https://www.justice.gov/eoir/foia-submit-a-request. The envelope and letter or email subject should be clearly marked "Privacy Act Access Request."

The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request should include a general description of the records sought and must include the

requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Although no specific form is required, individuals may use Form EOIR-59, Certification and Release of Records, available at https://www.justice.gov/eoir/eoir-forms.

More information regarding EOIR's procedures for accessing records is available at https://www.justice.gov/eoir/freedom-information-act-foia. General information about the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 C.F.R. Part 16 Subpart D, "Access to and Amendment of Individual Records Pursuant to the Privacy Act of 1974, and Other Privacy Protections."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in the system should direct their requests to EOIR at the address indicated in the ''RECORD ACCESS PROCEDURES'' paragraph above. All requests to contest or amend records must be in writing and the envelope, letter, or email subject should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. For general information regarding the Department's procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 C.F.R. 16.46, "Privacy Act Requests for Amendment or Correction."

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertaining to them is requested via the procedures identified in the "RECORD ACCESS PROCEDURES" paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(2), the Attorney General has exempted certain records of this system from subsections 5 U.S.C. 552a(c) and (d) of the Privacy Act.

Rules will be promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and will be published and codified in the Federal Register at 28 CFR 16.83.

HISTORY:

None.

[FR Doc. 2026-21062 Filed: 10/14/2026 8:45 am; Publication Date: 10/15/2026]