Executive Office for Immigration Review

Privacy Impact Assessment
for
Judicial Conduct 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: September 25, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

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

The primary mission of the Executive Office for Immigration Review (EOIR) is to adjudicate immigration cases by fairly, expeditiously, and uniformly interpreting and administering the Nation's immigration laws. Under delegated authority from the Attorney General, EOIR's administrative adjudicators[1] in the Office of the Chief Immigration Judge (OCIJ),[2] Board of Immigration Appeals (Board),[3] and Office of the Chief Administrative Hearing Officer (OCAHO)[4] conduct immigration court proceedings, appellate reviews, and administrative hearings. EOIR's Office of the Director (OOD), Judicial Conduct and Professionalism Unit (JCPU) implements a process for receiving, evaluating, and responding to complaints of inappropriate conduct by EOIR adjudicators. To this end, EOIR created the Judicial Conduct System (JCS), an electronic complaint management system designed to manage the adjudicator complaint process and lifecycle. The JCS generally handles adjudicator complaint information, such as complainant names and contact information; descriptions of alleged adjudicator conduct, including time and place of purported events; associated immigration case information, including alien registration numbers (A-numbers); and EOIR actions taken in response to complaints. The JCPU receives complaints and corresponds with complainants by email. Complaint records (including but not limited to additional or supporting complaint documents, investigatory notes, and notices) are stored and maintained in a configuration of on-premises and cloud-based servers. EOIR uses this information to investigate and take appropriate employment or other action in response to complaints of alleged adjudicator misconduct, professionalism, or ethics issues. Because the JCS collects, maintains, and disseminates personally identifiable information (PII), EOIR is conducting this privacy impact assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002.

---

[1] EOIR's administrative adjudicators include immigration judges (IJs), appellate immigration judges (AIJs) or Board members, and administrative law judges (ALJs)

[2] OCIJ is led by the Chief Immigration Judge, who establishes operating policies and oversees policy implementation for the immigration courts. OCIJ provides overall program direction and establishes priorities for approximately 600 immigration judges located across 68 immigration courts and three adjudication centers throughout the Nation.

[3] The Board is the highest administrative body for interpreting and applying immigration laws. The Board has been given nationwide jurisdiction to hear appeals from certain decisions rendered by immigration judges and by district directors of the Department of Homeland Security (DHS) in a wide variety of proceedings in which the Government of the United States is one party and the other party is an alien, a citizen, or a business firm.

[4] OCAHO is headed by a Chief Administrative Hearing Officer who is responsible for the general supervision and management of ALJs who preside at hearings which are mandated by provisions of law enacted in the Immigration Reform and Control Act of 1986 and the Immigration Act of 1990, both of which, among other laws, amended the Immigration and Nationality Act of 1952 (INA).

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 JCS is an electronic complaint management system for managing the judicial conduct complaint process and storing information pertaining to complaints against EOIR adjudicators. In the JCS, authorized users can: create a complaint file and enter complaint-related information; assign a unique numerical identifier to a complaint and record EOIR's actions in handling the complaint; track complaints throughout their lifecycle; record outcomes of complaints; generate summary reports of individual complaints; and create statistical reports depicting trends and aggregate complaint data.

The process begins when an individual or group submits a complaint[5] by mail or email to the JCPU. If the complaint suggests judicial misconduct,[6] the complaint is logged in the JCS, which assigns a unique complaint number and creates an electronic file for storing information and records associated with the complaint and any investigation. Once a complaint is docketed in JCS, the JCPU will review the complaint and any attachments, together with relevant agency records such as electronic records of proceeding, digital audio recordings, electronic docket entries, and electronic decisions. The JCPU then forwards the complaint, any attachments, and a summary of the JCPU's preliminary fact-gathering to the adjudicator's supervisor for further investigation and resolution, and the JCPU provides a copy of this communication to the EOIR Office of the General Counsel (OGC) Employee and Labor Relations (ELR) Unit.

Unless notification would compromise an ongoing investigation by another office or is contrary to law or agency-wide policy, the supervisor will promptly notify the adjudicator of the existence and substance of the complaint and give the adjudicator an opportunity to respond. However, if a complaint can be dismissed or concluded without the adjudicator's input and does not result in corrective or disciplinary action, the adjudicator may be informed of the existence of the docketed complaint at the same time they are notified that it has been resolved. If the allegations appear to fall under the jurisdiction of the DOJ Office of Professional Responsibility (OPR), the Office of the Inspector General (OIG), or the Office of the Special Counsel (OSC), EOIR will refer the complaint to those DOJ components for further investigation.

---

[5] A complaint is information that comes to the attention of EOIR suggesting that an adjudicator may have engaged in judicial misconduct.

[6] Judicial misconduct is conduct that may adversely affect the fair, effective, or expeditious administration of the work of EOIR's adjudicating components. Complaints that do not suggest judicial misconduct are handled appropriately outside of the JCPU process.

The supervisor's investigation of the complaint may involve reviewing agency records and soliciting statements from the complainant and any witnesses. If the supervisor finds that the allegations of misconduct are substantiated, the supervisor, in consultation with EOIR senior leadership and the ELR Unit, as appropriate, will determine whether and what type of corrective or disciplinary action is warranted.

Complaints are resolved with one of the following types of actions: dismissal, conclusion, corrective action, or disciplinary action. If the supervisor determines that the allegations in the complaint do not constitute judicial misconduct, the complaint will be dismissed. If the supervisor determines that intervening events, such as the adjudicator's retirement or resignation, render the complaint moot, or if corrective action has already been taken on the matter, the docketed complaint will be concluded on that ground. If the supervisor determines that non-disciplinary action is appropriate, the supervisor may consult with the EOIR OGC ELR Unit to determine the appropriate action, which may include counseling the adjudicator orally or in writing, consulting with senior leadership to arrange for individualized training, and/or initiating performance-based action. If the supervisor determines that disciplinary action is required, the supervisor will consult with ELR regarding the appropriate action, which may include a written reprimand, suspension without pay, or removal from federal service.

Once the investigatory and management process is completed, a complaint is resolved via final action. The JCPU will record the final action in the JCS and close the matter. A supervisor will notify the adjudicator once the matter is closed. The JCPU will notify the complainant in writing once the matter is closed. To promote transparency and accountability, EOIR periodically publishes aggregate program statistics on its website concerning the number of complaints and the final actions taken.

Only authorized EOIR personnel access the JCS on approved DOJ devices that require PIV credential authentication. Authorized personnel must be granted access by a system administrator. The system is currently connected to the EOIR Microsoft Azure Active Directory to verify whether a user is authorized to access, view, and/or edit data in the system. In future updates to the system, EOIR will be implementing measures to require PIV credential and multifactor authentication each time a user attempts to access the system.

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(g).
Executive Order	
Federal regulation	8 C.F.R. § 1003.0(b).
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	EOIR Policy Memorandum (PM) 19-14, *Allegations of Misconduct by EOIR Adjudicators and Ex Parte*

	Communications (Aug. 16, 2019); EOIR PM 21-15, *Adjudicator Independence and Impartiality* (Jan. 19, 2021); EOIR PM 25-02, *EOIR's Core Policy Values* (Jan. 27, 2025); EOIR PM 25-33, *Neutrality and Impartiality in Immigration Court Proceedings* (Jun. 27, 2025).

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 complainants and witnesses; names of EOIR adjudicators; names of EOIR personnel who are authorized users of the system.
Date of birth or age			
Place of birth			
Sex	X	C, D	Complainants may include their sex if relevant to the complaint.
Race, ethnicity, or citizenship	X	C, D	Complainants may include their race, ethnicity, or citizenship if relevant to the complaint.
Religion	X	C, D	Complainants may include their religion if relevant to the complaint.
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			

(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	A-numbers may be included in complaints or records of immigration proceedings impacted by the alleged conduct or reviewed during the course of an investigation.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal contact information, e.g., mailing address, e-mail address, phone number	X	C, D	Complainant and witness contact information may include a personal mailing address, email address, and/or phone number.
Business contact information, e.g., mailing address, e-mail address, phone number	X	A, B, C, D	Complainant and witness contact information may include a business mailing address, email address, and/or phone number. The system captures DOJ contact information of EOIR adjudicators, their supervisors, and EOIR personnel authorized to access the system.
Medical records number			
Medical notes or other medical or health information	X	C, D	Complainants may submit this information in forming the basis of their complaint and it may be collected by JCPU if relevant to the investigation.
Financial account information			
Applicant information	X	A, B, C, D	Unique numbers are assigned to each complaint and linkable to a particular adjudicator and complainant (except for complainants that submit anonymously). EOIRID numbers of attorneys or accredited representatives authorized to practice before EOIR may be included in complaints or witness statements. Applicant information from records of immigration proceedings impacted by the alleged conduct may be collected or reviewed if relevant to an investigation.
Education records			
Military status or other information			
Employment status, history, or similar information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A	The system stores information pertaining to disciplinary outcomes of complaints or employment actions taken in response to complaints, such as suspension dates.
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, C, D	Complainants may submit this information in forming the basis of their complaint and such information may be collected by JCPU if relevant to the investigation.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, C, D	Complainants may submit this information in forming the basis of their complaint and it may be collected by JCPU if relevant to the investigation. The JCPU may access underlying records of immigration proceedings (civil administrative proceedings) if relevant to the investigation.
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			

(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
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	User ID or PIV credential of EOIR personnel authorized to access the system.
- **User passwords/codes**	X	A	User password or PIV credential of EOIR personnel authorized to access the system.
- **IP address**	X	A	IP address of EOIR personnel authorized to access the system.
- **Date/time of access**	X	A	User access and activity and date/time of user access and activity of EOIR personnel authorized to access the system.
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Although EOIR anticipates the above categories of PII, it is possible that other types of PII may be included in complaints, witness statements, and associated immigration court records. Given the varied nature of complaints and the fact that complainants voluntarily provide information they deem relevant to the complaint, it is not possible to identify all of the possible categories of PII that could be collected.

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): Complaints are received by mail or email.					

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 a complaint.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Anyone may submit a complaint. The JCPU may initiate a complaint based on information discovered through news articles or public media available on the Internet.					

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			Relevant information is provided on a case-by-case basis to the following EOIR personnel and components as part of the adjudicator complaint process: to the adjudicator's supervisor(s); to EOIR senior leadership; and to the OGC ELR Unit. Information is provided to the EOIR OGC Freedom of Information Act (FOIA) Unit on a case-by-case basis if necessary to respond to a FOIA request. Information is also provided to the EOIR OGC Attorney Discipline Unit on a case-by-case basis if the complaint suggests a violation of the rules of professional conduct for immigration practitioners representing clients in EOIR immigration proceedings. Aggregate information may be provided to the EOIR Office of Policy for purposes of developing trainings.
DOJ Components	X			Based on the nature of the complaint, relevant information may be shared on a case-by-case basis with the DOJ Office of Professional Responsibility, the Office of the Inspector General, or the Office of Special Counsel. Information may also be shared on a case-by-case basis with the Office of the Attorney General for purposes of evaluating whether to convert an adjudicator from a probationary to a permanent position.

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			If relevant to administrative proceedings or otherwise required by law or administrative order, information in the system may be shared with the Merit Systems Protection Board or the Equal Employment Opportunity Commission. Relevant, aggregate information may be shared on a case-by-case basis to complete mandatory reports to Congress.
State, local, tribal gov't entities				
Public	X			Aggregate, de-identified statistics on adjudicator complaints are published on EOIR's public website. Members of the public may request information pursuant to the Freedom of Information Act (FOIA) or Privacy Act (PA), subject to applicable exemptions.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Adjudicators who are subjects of complaints, or their designated counsel or representative, may receive access to specific information in the system pertaining to them. If determined relevant to judicial proceedings or otherwise required by law or court order, information in the system may be shared with judicial tribunals for litigation purposes.
Private sector				
Foreign governments				
Foreign entities				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Other (specify):	X			The JCPU notifies complainants to acknowledge receipt of complaints and to notify when the complaint has been closed. The JCPU may share limited information with others during the investigation process if necessary to substantiate or verify complaints or allegations.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

EOIR makes immigration judge complaint statistics available to the public on the EOIR Statistics and Reports website and on data.gov. To protect individual privacy, EOIR de-identifies and aggregates the data prior to publication.

Section 5: Notice, Consent, Access, and Amendment

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

EOIR publishes the complete adjudicator complaint process on its website, Complaints Regarding EOIR Judges, which informs individuals about how the JCPU collects, uses, shares, and otherwise processes PII as part of this process. EOIR also employs several other methods to generally notify and inform individuals how the agency collects, uses, shares, and processes their PII: (1) SORNs published in the Federal Register and available for convenience on the DOJ website (https://www.justice.gov/opcl/doj-systems-records#); (2) Privacy Act § 552a(e)(3) notices on EOIR information collections and public-facing applications that collect PII; and (3) the DOJ Privacy Policy, displayed on the common footer of the EOIR website (https://www.justice.gov/doj/privacy-policy).

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Complainants and witnesses voluntarily provide nearly all of the information submitted as part of a complaint, statement, or correspondence recorded in the JCS. While PII is not required to submit a complaint, complaints generally include at least the name of the subject of the complaint, along with other potentially identifying information, such as the time and place of the incident giving rise to the complaint. Complainants and witnesses may decline to provide information to the JCPU; however, failure to provide information may hinder the complaint investigation process.

Unless notification would compromise an ongoing investigation by another office or is contrary to law or agency-wide policy, the supervisor will promptly notify the adjudicator of the existence and substance of the complaint and give the adjudicator an opportunity to respond, providing the adjudicator with an opportunity to voluntarily participate in the collection of information. However, if a complaint can be dismissed or concluded without the adjudicator's input and does not result in corrective or disciplinary action, the adjudicator may be informed of the existence of the docketed complaint at the same time they are notified that it has been resolved.

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.

Complainants may receive confirmation via email of whether an investigation is ongoing or whether the complaint is resolved.

Subjects of complaints may receive or request copies of information about themselves through their management chain as part of the investigation process. Subjects may offer corrections or amendments to information to their manager as part of the investigation process, and such submissions are added to a complaint file.

Otherwise, individuals may submit a Freedom of Information Act (FOIA) request or a Privacy Act access or amendment request with EOIR's FOIA Office. Instructions for making such requests are available on the EOIR website (https://www.justice.gov/eoir/freedom-information-act-foia). Individuals may also follow the record access and amendment procedures described in applicable SORNs identified in Section 7 of this PIA.

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):** JCS operates under the JCON/eWorld – Adjudication Support ATO, most recently granted on August 29, 2025, and expiring on August 29, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no outstanding POAMs for any privacy controls.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** EOIR has assigned a FIPS 199 security categorization of Moderate.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** In accordance with DOJ Order 0908, *Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information*, and to protect EOIR's data from spills, leaks, and/or misuse, EOIR performs daily monitoring of cybersecurity incidents, continuously evaluates alerts for cyber threats, and conducts annual cybersecurity incident response testing.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** EOIR collects and maintains audit logs for 120 days and reviews audit logs weekly to ensure compliance with security and privacy standards.

X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** To ensure new personnel understand how to properly use the system, JCPU provides new personnel with copies of written procedures and live demonstrations of the system.

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

Access to JCS is limited to authorized EOIR employees and contractors responsible for conducting complaint investigations or as system administrators. User permission and access to information in the 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 DOJ Rules of Behavior regarding use of DOJ/EOIR information systems.

EOIR user accounts are reviewed annually to determine whether continued access is necessary, and user 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.

EOIR conducts regular vulnerability scanning and configuration management activities to minimize privacy and security risks associated with the receipt of email complaints and any attachments included with email complaints.

System and user activity is regularly monitored, logged, and audited to detect suspicious activity. Data 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.

System data and records, including information stored in associated network drives, are backed up regularly and stored according to applicable record retention schedules and policies.

Before complainant or witness information is disclosed or disseminated, the JCPU reviews all information and masks, removes, or redacts PII in accordance with law and any requests received from complainants or witnesses to anonymize their identity. Before EOIR disseminates statistical data generated from the JCS, EOIR deidentifies and aggregates the data to protect the privacy of complainants, witnesses, and adjudicators.

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.

Some records in this system are scheduled under the EOIR Immigration Judge Complaint Files Schedule (N1-060-09-6). Immigration judge complaint files and records are temporary records cut off at the end of the calendar year after the employee leaves the position as an immigration judge and destroyed/deleted three years after cutoff of when no longer needed for business purposes, whichever is later. The master file for the EOIR Immigration Judge Complaint System (E-IJCS) maintained by EOIR OCIJ is a permanent record, cut off at the end of the calendar year after the employee leaves the position as an immigration judge and transferred to the National Archives in five-year blocks 10 years after cutoff of the most recent records in the block.

To the extent that any JCPU records or records in the JCS are unscheduled, EOIR retains such records indefinitely until 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:

OPM-GOVT-3, Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, 71 FR 35350 (Jun. 19, 2006); 87 FR 5874 (Feb. 2, 2022); https://www.opm.gov/information-management/privacy-policy/#url=SORNs.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and

how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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

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

There is a risk that the system inadvertently collects more information than may be necessary for JCPU to conduct the adjudicator complaint investigation process, including PII about third parties who do not have an opportunity to consent to the inclusion of their information. The JCPU does not restrict the amount or type of information that individuals may include in complaints, including any PII voluntarily included by the complainant. To mitigate this risk, several notices are provided to proactively inform and remind the individual that they voluntarily choose the information to include in complaints, how such information may be used by the agency, and how the individual may request confidentiality or anonymity of their information or identity. These notices are described in Section 5 of this PIA. When interviewing witnesses or collecting witness statements, EOIR employees investigating the complaint attempt to limit the information collected from the witness by asking questions designed to elicit only information that is relevant and necessary to investigate a complaint.

The JCS and associated network drives maintain significant quantities of PII, and the agency must likewise exert significant efforts to ensure the PII is accurate and reliable. Throughout the investigation process, EOIR verifies the accuracy and reliability of complaint information and includes additional findings to the complaint file to ensure it stays up to date throughout the investigation process. Otherwise, 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, all of which are described in Section 5.3 of this PIA. Names and complaint numbers are the primary means by which the JCPU retrieves information in this system; records maintained with an inaccurate name or complaint number could result in improper disclosure of PII or associate incorrect information with a particular name or complaint number. For this reason, the JCPU marks all related records with the same complaint number, and the JCS has the ability to link multiple complaint numbers when the JCPU determines that separate complaints were docketed for the same conduct or event.

The JCPU may receive numerous complaints from a variety of sources. Given the volume, varied

nature, and sensitivity of such complaints, EOIR must carefully monitor access and use of the information to protect against unauthorized activity. EOIR mitigates this risk by only granting access to employees and contractors who complete the requisite security clearance, identity validation, and annual security and privacy training, and who annually review and acknowledge DOJ's Rules of Behavior to maintain system access. System access and activity are all restricted to users with an authorized need to know, and permissions are tailored to the particular user's role. User accounts are reviewed regularly and deactivated after a specified period of inactivity. Moreover, user activity audits are conducted regularly to monitor suspicious activity. Several virtual and physical security measures are in place to safeguard information, including IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and audit logs. System hardware, such as servers, are located in secure facilities. Data is also encrypted in transit and at rest.

The JCPU shares complaint information with a variety of recipients for different purposes, which increases the risk of inadvertently spilling PII to the incorrect recipient. Judicial complaint files and records are appropriately and clearly marked with unique complaint numbers and filenames for easy and accurate cross-referencing of information across all record storage locations. Before sharing any records or complaint information, JCPU personnel manually review and confirm that the contact information included on correspondence belongs to the intended recipient of the information. The JCS includes a unique marker to indicate when a complainant requests that their identity remain anonymous; JCPU personnel inform complainants how their anonymity may impact investigation or resolution of the complaint and inform complainants that they may waive confidentiality. When fulfilling requests for statistical data or publishing statistical data to its website, EOIR aggregates the data to ensure the data does not identify any particular individual.

While most of the records in this system fall under a published disposition schedule, EOIR's record retention schedule for records maintained in the JCS does not capture all record types generated or captured in the system; therefore, some records in the system are unscheduled and must be retained indefinitely. The longer that EOIR retains information about individuals, the more opportunities exist for a spill or breach of that information. Such risk will be mitigated once EOIR updates its existing record retention schedule in a manner that permits EOIR to appropriately dispose of all record types stored in the system or on associated network drives.