

Civil Rights Division



Privacy Impact Assessment for the Immigrant and Employee Rights Charge Form

Issued by:
John Buchko

Senior Component Official for Privacy

Approved by: Andrew J. McFarland
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 25, 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 Civil Rights Division (CRT) intends to modify the way in which the public can file complaints with the Immigration and Employee Rights Section (IER) of the U.S. Department of Justice, alleging employment discrimination based on citizenship status or national origin, as outlined in the Immigration and Nationality Act (INA). To do so, CRT is redesigning the existing IER Charge Form (Form).

The Form will collect the same information as the [legacy form](#), but will be revised for better use and mobility within CRT and, by moving it to a more modern platform, it will become mobile-friendly for easier use by the public. The revised Form will also utilize U.S. Web Design System (USWDS) components to improve accessibility and be Form 508 compliant. The system will include personally identifiable information, such as names, emails and phone numbers, as well as employment information and medical information. Due to the nature of the complaints, it may also capture additional sensitive information.

The Form will be using Amazon large language models (LLMs), natural language processing (NLP) and Generative artificial intelligence (AI) Services to assist CRT employees to group and label reports as well as understand what data might be missing from reports submitted by the public. The AI will not communicate with the public or take action on any report.

DOJ contractors and designated Need-to-Know CRT IER employees will have access to this system. Some reports created within this database will be shared with other DOJ components or federal agencies for the purpose of referral to a more appropriate source of support for a claim.

CRT is conducting a privacy impact assessment because the revised Form electronically collects information provided to CRT by members of the public with their contact information (name, email, phone, etc.) and describes what they witnessed, capturing potentially sensitive volunteered information. While the information provided will be the same as the legacy form, the storage and additional uses for more effective complaint management implicate, consistent with the eGovernment Act of 2002, information in identifiable form from or about members of the public. The Form is consistent with the Paperwork Reduction Act.

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 project is designed to 1) improve use of and purpose for CRT employees and 2) make the Form more user friendly for the public. The Form is being moved from the legacy Oracle platform to a new host in the more modern Cloud.gov environment¹ and stored in a Postgres database². After the move, CRT will implement the GovDelivery³ email system that will automatically send users a confirmation email with a unique record number for their submission and will also provide CRT the ability to send form letter responses to the public.

The Form will be using Amazon LLMs, NLP and Generative AI Services to assist CRT employees to group and label reports as well as understand what data might be missing from reports submitted by the public. The AI will not communicate with the public or take action on any report.

CRT intake specialists will have the ability to mark the status of the report, reassign it to other intake specialists, refer reports to other agencies and as mentioned, reply to the public.

While only need-to-know CRT employees and contractors will have access to the database, information may be exported from the database to share with other DOJ components, contractors, federal agencies, entities or individuals as deemed necessary for coordination on investigations and litigations or to refer information to a more appropriate DOJ component or federal agency for support and response. However, access to the database will not be shared with them.

2.2 *Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

The Form is used to file a complaint with CRT's IER, which has legal authority to address allegations of employment discrimination based on citizenship status or national origin, as outlined in the INA. IER enforces the anti-discrimination provision of the INA, 8 U.S.C. § 1324b. Regulations for this law are found at 28 C.F.R. Part 44.

Authority	Citation/Reference
Statute	8 U.S.C. §1324b
Executive Order	

¹ Cloud.gov is a FedRAMP approved Platform-as-a-Service (PaaS) within the General Services Administration (GSA).

² Postgres is a relational database.

³ GovDelivery is covered under separate privacy documentation.

Federal regulation	28 C.F.R. Part 44
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

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
<i>Example: Personal email address</i>	<i>X</i>	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	X	C	Name (optional), Name of Employer, Possible Names of Witnesses in Description
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship	X	C	Citizenship Status
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C&D	Alien Number/UCIS Number
Passport number			
Mother's maiden name			

Department of Justice Privacy Impact Assessment
[CRT/Immigration and Employee Rights Charge Form]
Page 4

(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
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	C	Email (optional), business contact information (city, state, mailing address)
Personal phone number	X	C	Phone number (optional)
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
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			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
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			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
<i>Biometric data:</i>			
- Photographs or photographic identifiers			
- 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)			
<i>System admin/audit data:</i>			CRT Need-to-Know Component Employees responsible for administering and auditing the system have access to the content of the files in the system. While reports may be sent to other DOJ components or federal agencies, they will not have access.
- User ID			
- User passwords/codes			
- IP address			
- Date/time of access			
- Queries run			
- Contents of files			
Other (please list the type of info and describe as completely as possible):	X	C&D	Injured Party's Citizenship or Immigration Status Information

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): The Form also provides a hard copy, email and fax option for sending charges. Once received Need-to-Know IER employees will input the information into the database.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

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	
Within the Component			X	- This information is shared with Need-To-Know CRT employees and contractors. Methods used are directly from the public or from CRT employees and contractors who receive complaints via email, fax and hard copy. - Staff are trained on how to properly handle sensitive information. Rules

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	
				of behavior and nondisclosure agreements are required for all users before access is provided. Access to the system is safeguarded by the use of PIV cards. CRT staff also receive annual computer security awareness training regarding how to properly protect PII in accordance with Department of Justice standards. • Security controls commensurate to the National Institute of Standards and Technology-Federal Information Processing Standards Publications No. 199, "Standards for Security Categorization of Federal Information and Information Systems," are in place for CRT JCON. CRT adheres to the Department's Risk Management Framework (RMF) and creates a System Security Plan that will ensure CRT follows strict DOJ NIST 800-53 Rev 4 core control standards. • If CRT staff may need to share a particular report of a violation with another DOJ component – for example, if CRT is coordinating with another DOJ component on litigation where a report of a violation is relevant – CRT does not intend to allow access directly. CRT personnel would duplicate and share a copy of the relevant report with known personnel of that DOJ component, with all applicable protections for PII.
DOJ Components	X			Information will be exported and shared for the purposes of investigation, litigation and referral via secured DOJ communications networks.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	
Federal entities	X			Information will be exported and shared for the purposes of investigation, litigation and referral via secured federal communication networks
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
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.*

This information will not be released for **Open Data** purposes.

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.*

In accordance with the Privacy Act, a (e)(3) notice will appear on the Form where information is being collected.

As with the legacy Form, this revised Form will have the following Privacy Act Statement:

The authority for requesting this information from the Injured or Charging Party is contained in 8 U.S.C. § 1324b. The information that the Injured or Charging Party provides will be used principally for investigating and processing the charge of prohibited discrimination; however, the information may also be used for other legitimate purposes, as detailed in the Department of Justice's Federal Register Notice published in the Federal Register at 68 Fed. Reg. 47611 (August 11, 2003) describing the routine uses of the information obtained by the Civil Rights Division. While completing the form is voluntary, the Injured or Charging Party's failure to provide the information requested on this form could lead to the charge being dismissed or not being accepted. Knowingly making false statements on this form is punishable under 18 U.S.C. § 1001.

The names and contact information maintained in this system for the purpose of investigating allegations of employment discrimination are covered by the CRT SORN titled: JUSTICE/CRT-001, "Central Civil Rights Division Index File and Associated Records." Additional general notice is within this PIA, if published.

Any AI learning/processing would happen on a dedicated CRT server - meaning information is not being shared with public AI models.

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 will have the opportunity to decline to volunteer some information in the form but will not have the opportunity to choose which parts of the Form they consent to possible disclosure.

The final section of the Form is an Affirmation, where the user (injured party or authorized representative) is notified that by submitting the Form, they are consenting to the information provided possibly being disclosed during an investigation, legal proceedings or possibly in response to a Freedom of Information Act request.

Individuals are not obligated to provide a report through the Charge Form if they do not want to complete any required fields. They have the option of submission via fax, regular mail or email. Moreover, most fields in the public-facing Form are optional for users. Finally, before submitting a report to CRT via the Form, users have a chance to review the report and make changes before submission.

There is no opt-out of AI/ML with respect to their information and there are no alternatives for processing information submitted that do not include the routine use of AI in the system.

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 access to information in the system pertaining to them is governed by the CRT SORN titled: JUSTICE/CRT-001, "Central Civil Rights Division Index File and Associated Records." Disseminating records to complainants and victims in compliance with The Privacy Act is a routine use provided in the SORN. Additionally, procedures for "Record Access" and "Contesting Records" are detailed in the SORN, allowing individuals to access, request amendment or corrections to their information. Individuals may also follow the procedures outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations.

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).*

	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): We are operating under the CRT-CP. The CRT-IER system operates within the same security boundary utilizing the same NIST 800-53 Rev 5 controls. If an ATO has not been completed, but is underway, provide status or expected completion date: We are operating under the CRT-CP. The CRT-IER system operates within the same security boundary utilizing the same NIST 800-53 Rev 5 controls. Expected completion date is August 1, 2026. 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: NO POA&Ms are currently active.
	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:

	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 data is stored on Cloud.gov, which is FedRAMP Medium. This system did not require FedRAMP High because the data, if breached, would not have a severe or catastrophic adverse effect on agency operations, organizational assets, or individuals.
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: All applicable NIST 800-53 Rev5 controls have been reviewed, tested and fully assessed. CRT follows the JMD's Security and Privacy Assessment and Authorization Handbook Appendix H – Information Security Continuous Monitoring (ISCM) Plan.
	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: Cloud.gov ensures compliance with security and privacy standards by collecting system logs which are reviewed through a centralized log dashboard. The security analyst reviews the logs every week and notifies CISO if any unauthorized access detected.
	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. All CRT employees (federal and contractor) are required to complete the annual Cybersecurity Training, including employees with privileged accounts, and must complete the annual IT Professional Training. All training completions are reported to JMD.
	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: All CRT employees (federal and contractor) are required to complete privacy training when on-board as well as complete the annual Cybersecurity Training which includes signing the department's Cybersecurity and Privacy Rules of Behavior.

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?

To mitigate privacy risk, access to the system is limited to only need-to-know employees and contractors. The system will incorporate all required federal standards for information security for this level of information. Staff are trained to properly handle sensitive information. Non-disclosure agreements have also been carried out to ensure proper use and protection of sensitive information. Access to the system is safeguarded using personal identity verification (PIV) cards and/or RSA tokens. CRT staff also receive annual computer security awareness training regarding how to properly protect PII in accordance with Department of Justice standards.

Security controls commensurable to the National Institute of Standards and Technology-Federal Information Processing Standards Publications No. 199, "Standards for Security Categorization of Federal Information and Information Systems", are in place. CRT adheres to the Department's Risk Management Framework (RMF) and creates a System Security Plan that will ensure CRT to follow strict DOJ NIST 800-53 Rev 5 core control standards.

When disseminating PII, is information encrypted in transit?

All PII information is encrypted in transit.

How does the system detect potential unauthorized access to the system?

System log both authorized and unauthorized access. All unauthorized access is monitored via log review.

Does the system require users to use two-factor authentication to gain access to the system?

Yes, 2FA and Multi-FA are enabled by mandatory PIV PIN, DOJ Login OKTA zero trust and active DOJ account.

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.*

The records in the Form are retained in the database while current and required for official Government use. For final disposition, CRT intends to adhere to the records retention policy approved by NARA. If CRT associates a report with a specific matter or case, the official record of the report becomes part of that matter or case file, subject to the appropriate records retention schedule approved by NARA.

ONE YEAR (DAA-0060-2014-0004-0002)

Public Correspondence – No Response: Documents that do not include any communications to which CRT replies to the submitter or refers to another component/agency.

- Disposition Method: Manually deleted from the system (any accompanying hardcopy records destroyed).

THREE YEARS (DAA-0060-2014-0004-0002)

Public Correspondence – Response Required: Documents that require a routine response but lack evidential value and require no policy decisions or administrative actions.

- Disposition Method: Manually deleted from the system (any accompanying hardcopy records destroyed).

TEN YEARS (DAA-0060-2017-0022-0002)

General DJ Number Temporary Files (GNT) – Correspondence or materials that have not developed into a matter or case handled by the Department of Justice, require few or no action and document only routine administrative, statistical, or reporting actions for the DJ Class. If a DOJ-handled case or matter later develops out of the material, the section responsible for the records will open a formal DJ numbered case and move (or copy) material from the database into the DJ numbered case file. The official record of the report becomes part of that matter or case file and is subject to the appropriate records retention schedule approved by NARA for the DJ Class.

- Disposition Method: Manually deleted from the system (any accompanying hardcopy records destroyed).

TWENTY-FIVE YEARS (DAA-0060-2017-0022-0001)

General DJ Number Permanent Files – (GNP) – Correspondence or materials that document CRT's direction for litigation activities within the DJ Class. Records with a GNP designation are permanent records, and such records would not be stored in the system.

- Disposition Method: CRT requests for a transfer of records to NARA. Once NARA confirms legal possession of records, they are manually deleted from the system where they are located (and accompanying hardcopy records destroyed).

AI learning/processing would happen on a dedicated CRT server - meaning information is not being shared with public AI models.

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:*

The records on this Form are governed by a previously published SORN titled: JUSTICE/CRT-001, “Central Civil Rights Division Index File and Associated Records.” The SORN and all its citations and amendments can be found here: <https://www.justice.gov/opcl/doj-systems-records#CRT>.

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.

CRT only collects information that is relevant to the IER charge, which is collected directly from the public submitter. There is no way for individuals to opt out of sharing certain information once the Form has been submitted. DOJ’s web privacy policy is listed on the IER form. The public facing form, which is built in python/Django, takes information in and the data submitted is stored on Cloud.gov in a Postgres database. Cloud.gov is compliant with more than 155 of the NIST 800-53 Rev 5 controls and aligns with Zero Trust Executive Order 14028. In the future, we may add LLM and NL AI functions to sort incoming reports and help us identify what is missing from reports.

If CRT staff may need to share a particular report of a violation with another DOJ component – for example, if CRT is coordinating with another DOJ component on litigation where a report of a violation is relevant – CRT does not intend to allow access directly. CRT personnel would duplicate and share a copy of the relevant report with known personnel of that DOJ component, with all applicable protections for PII, such as encryption in transit. Information will only be shared with other DOJ components and federal agencies when it is on a need-to-know basis for the purposes of referral, investigation or litigation.

CRT Privacy and Cybersecurity officials are monitoring any security and privacy administrative, technical, and physical controls over the information. With all technology in use, the risk is exposed PII, but data will be stored on a secure CRT-specific server. We will use fictional CRT reports and show the AI model what data is missing. This training will help the model identify missing data from future incoming reports.