



DEPARTMENT OF JUSTICE

[CPCLO Order No. 003-2026]

Privacy Act of 1974; Systems of Records

AGENCY: United States Department of Justice, Civil Rights Division (CRT or the Division).

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974 (5 U.S.C 552a), CRT proposes to establish a new system of records titled “Civil Rights Division Reporting Portal,” JUSTICE/CRT-012. This system of records modernizes how the Division receives reports of alleged civil rights violations from the public. It operates as a web application and database where the public will be able to access a streamlined, responsive web form to report potential violations of federal civil rights laws and securely submit the completed form to the database. The system also allows CRT to add reports received through non-web channels, such as hardcopy mail, telephone, email, or fax to the portal’s database. This system enables the Division to more efficiently review and process reports to determine whether a report may contain information that supports further inquiry by CRT or pertains to ongoing investigations and legal proceedings on various issues related to protecting civil rights. This system will also allow the Division to provide status updates to the public, track portal metrics, and analyze progress on the concerns raised by the reports.

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. Please submit any comments by [INSERT DATE 30 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, 145 N St. 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: Randy Abramson, Product Manager, Civil Rights Division, 950 Pennsylvania Avenue, NW, Washington, DC 20530-0001, 202-598-9631.

SUPPLEMENTARY INFORMATION: To assist in carrying out its mission of protecting the civil rights of all people in the United States, the Division established the Civil Rights Division Reporting Portal. The Portal provides individual members of the public with easy access to a user-friendly process to report, in detail, potential allegations of federal civil rights violations via a web application form, and to submit the completed form to a secure database. While the reporting form requests some personal data, such as the name, address, email, etc. of the individual completing the report, it does not ask for identifying numbers, such as social security or employee identifiers. Individuals will have the opportunity to decline to provide some forms of information and to review their reports before submitting them. Members of the public will only have access to information about their own reports within the system. They will not have access to the database or be able to view reports of others.

Authorized CRT employees will use the system to open and close reports, as well as to assign, review, search, group, reroute, and track reports. The system can also be used to communicate with members of the public who submit reports.

Where appropriate and authorized by law, CRT employees will use reports/records in this system for the following purposes:

- 1) Internal Processing: Sorting, filtering or searching of reports for ease of analysis and processing.
- 2) Civil enforcement activities: Initiating a new investigation or adding to an ongoing investigation.
- 3) Criminal enforcement activities: Direct victims and/or witnesses of potentially criminal conduct to contact the appropriate law enforcement agency or forward to CRT's Criminal Section.
- 4) Litigation: If a report relates to ongoing litigation, the record may be used in that litigation.
- 5) Disposition: Following CRT records retention guidelines. CRT employees designate a time when reports are to be removed from the system. Once removed, the reports are permanently deleted from the system. In other cases, reports are sent to NARA pursuant to the requirements of the Federal Records Act.
- 6) Public Communications: CRT employees may use the system to reply to and communicate with the public via e-mail, physical mail or phone. Employees may also use the system to educate the public on CRT enforcement areas and redirect, when possible, to better resources outside of CRT. Finally, the system may be used to provide status updates to the individual members of the public on their reports.

This system will be included in the CRT's inventory of record systems.

April 23, 2026
Date

Peter A. Winn
Chief Privacy and Civil Liberties Officer (Acting)
United States Department of Justice

JUSTICE/CRT-012

SYSTEM NAME AND NUMBER: Civil Rights Division Reporting Portal,

JUSTICE/CRT-012

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Access to these electronic records includes all department locations that CRT operates or that support CRT operations, including U.S. Department of Justice, Civil Rights Division, 950 Pennsylvania Avenue, NW, Washington, DC 20530-0001.

SYSTEM MANAGER(S): Amanda Bryce, Chief Information Officer, Civil Rights Division, 950 Pennsylvania Avenue, NW, Washington, DC 20530-0001, 202-305-5323, Amanda.Bryce@usdoj.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The records in this system of records are kept under the authority of the following statutes: Official Misconduct, 18 U.S.C. §§ 241, 242; The Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act of 2009; Federally Protected Activities, 18 U.S.C. § 245; Criminal Interference with Right to Fair Housing, 18 U.S.C. § 3631; Damage to Religious Property, 18 U.S.C. § 247; Trafficking Victims Protection Act (TVPA); Freedom of Access to Clinic Entrances Act (FACE); Criminal Protection for Voting Rights, 18 U.S.C. § 594; Americans with Disabilities Act, Title I; Americans with Disabilities Act, Title II; Americans with Disabilities Act, Title III; Rehabilitation Act of 1973; Civil Rights Act of 1964, Title VII; Uniformed Services Employment and Reemployment Rights Act (USERRA); Civil Rights Act of 1964, Title IV; Equal Education Opportunities Act of 1974 (EEOA); Individuals with Disabilities in Education Act (IDEA); Civil Rights Act of 1964, Title VI; Education Amendments of 1972, Title IX; Civil Rights Act of 1964, Title II; Fair Housing Act (FHA); Equal Credit Opportunity Act (ECOA); Religious Land Use and Institutionalized Persons Act (RLUIPA); Servicemembers Civil Relief Act (SCRA);

Immigration and Nationality Act § 274B; Civil Rights of Institutionalized Persons Act (CRIPA); Violent Crime Control and Law Enforcement Act § 14141; Omnibus Crime and Safe Streets Act; Voting Rights Act; Voting Accessibility for the Elderly and Handicapped Act; Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA); National Voter Registration Act (NVRA); Genetic Information Nondiscrimination Act (GINA), Title II; Help America Vote Act (HAVA); Civil Rights Acts of 1870, 1957, 1960, & 1964.

PURPOSE(S) OF THE SYSTEM: The system has two primary purposes: 1) to provide a clear and seamless resource for members of the public to report to CRT suspected violations of federal civil rights laws; and 2) to provide CRT with a more efficient way to review and process reports and determine whether the report may contain information that supports further inquiry by CRT or pertains to ongoing investigations and legal proceedings on various issues related to protecting civil rights. In addition, the system will have the following functions:

- a. Searching: Finding reports based on specific dates, keywords, personal descriptions, section, contact information and more.
- b. Grouping: Grouping reports based on similar data, such as - by repeated writers, incident locations and offenses. Using advanced programming to group common reports.
- c. Analysis: Using contracted information technology services, including Artificial Intelligence (A.I.) services. Any data processed by such contracted information technology services will take place in a secure environment that satisfies all Departmental privacy and security standards.
- d. Cross System Referencing: Take in reports from other DOJ divisions. Refer reports to other agencies with more appropriate jurisdiction and eventually track

reports that develop into cases within the Civil Rights Division's main case management tool.

e. Communication: Reply to and communicate with individual members of the public on report status, additional resources, and enforcement.

Note: Items (b) & (c) are for the purpose of identifying violation trends.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals about whom records are maintained in this system may include individuals who are the subjects of investigations, as well as victims, potential witnesses, representatives of individuals and organizations, who have provided information about subjects directed to or referred to CRT, as well as other individuals and organizations referred to CRT in potential and actual cases and matters.

CATEGORIES OF RECORDS IN THE SYSTEM: Records in this system contain information provided by:

- Members of the public, including their contact information: name, address, phone number and email address, together with details about the witnessed violation.
- Memoranda, correspondence, studies, and reports related to enforcement of civil rights laws and other various duties of CRT.

RECORD SOURCE CATEGORIES: Records in this system are obtained from two sources. Primarily, from members of the public who create a record through completion and submission of the reporting form. Additionally, CRT employees will create records by adding new reports from the public sent via non-web sources (fax, mailed letters, emails, phone or other DOJ components and federal agencies) as well as adding comments and updates to existing reports.

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 the exceptions to the non-disclosure provisions of 5 U.S.C. 552a(b), when otherwise compatible with the purposes for which the records were collected or created, the records contained in this system of records may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) for the purposes described below:

(1) In the event that a record indicates a violation or potential violation of law – criminal, civil, or regulatory in nature – it may be referred to the appropriate federal, state, local, foreign, or tribal law enforcement authority, or to other agencies charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(2) To a federal, state or local agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information or has the expertise in an official or technical capacity to assist in the administration of a federally mandated program or the investigation or litigation of a case or matter, in order to analyze information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such assistance, information or expert analysis, or to obtain the cooperation of a prospective witness or informant.

(3) In connection with an appropriate proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative tribunal, when the Department of Justice determines that the records are arguably relevant to the proceeding, or the adjudicator determines the records to be relevant to the proceeding.

(4) To an actual or potential party to litigation or the party's attorney (a) for the purpose of negotiation or discussion on such matters as settlement of the case or matter or plea bargaining, (b) in connection with formal or informal discovery proceedings or to issue a Notice of Right to Sue letter upon request of the actual or potential party or upon a decision not to initiate an investigation or litigation.

(5) A record relating to a case or matter that has been referred for investigation or for issuance of Notice of Right to Sue, may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any determination that has been made.

(6) A record relating to a person held in custody or probation during a criminal proceeding or after conviction may be disseminated to any agency or individual having responsibility for the maintenance, supervision, or release of such person from custody or probation.

(7) A record may be disseminated to the United States Commission on Civil Rights in response to its request and pursuant to 42 U.S.C. 1975(d).

(8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

9) To mediators, negotiators or other persons engaged in efforts to resolve or settle cases or matters pending in CRT as is necessary to enable them to perform their assigned duties.

(10) To complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim.

(11) To Members 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, individual constituents who are subjects of CRT records.

(12) To the National Archives and Records Administration (NARA) and to the General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(13) 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.

(14) To any person or entity that CRT has reason to believe possess information regarding a matter within the jurisdiction of CRT, to the extent deemed to be necessary by CRT to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

(15) 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 relevant and necessary to the recipient agency's decision.

(16) 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.

(17) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) 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 (3) 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.

(18) 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 (1) responding to a suspected or confirmed breach, or (2) 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.

(19) 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.

(20) To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: CRT stores records in this system electronically. The data collected by the web application is stored and managed in a secure cloud-based database. The database is set up for automatic backup.

Logs created by the web app are automatically captured in Cloud.gov. Static assets for the app are stored in Cloud.gov's Amazon Web Services (AWS) Simple Storage Service.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: CRT employees will access the records in this system via a search engine using various identifiers such as name, location, system-generated report number assigned at the time of submission, or other keywords.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: Records are retained on the system while current and required for official Government use. Final disposition is in accordance with records retention schedules approved by NARA. If CRT associates 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).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: CRT safeguards records in this system according to applicable rules and policies, including all applicable Department of Justice automated systems security and access policies. Both the app and database are stored and managed on a secure and encrypted cloud-based server. A security risk assessment has been conducted and auditing procedures are in place. CRT has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permission. The delegated legal duties and responsibilities of each section of CRT are described in detail at the Division’s website:

<https://www.justice.gov/crt>. CRT employees will access the database using a password-protected, cloud-based interface. To protect the confidentiality of the data, the system is integrated with the DOJ's single sign-on, so that all authenticated views are compliant with DOJ account policy and provide PIV sign on tracking.

If CRT needs to share a particular report with another DOJ component or agency – for example, if CRT were coordinating with another DOJ component on litigation where a report of a violation is relevant – CRT personnel would duplicate and share a copy of the relevant report with known personnel of that DOJ component, with all applicable protections for personally identifiable information. As noted above, the official record of the report would become part of the case or matter file, and the report remaining in the system would be a reference or convenience copy, destroyed when no longer needed.

RECORD ACCESS PROCEDURES: Individuals seeking access to, and notification of, any record contained in this system of records, or seeking to contest its content, may submit a request in writing to CRT's Chief Privacy and Freedom of Information Act Officer, Kilian Kagle, FOIA/PA Branch, Civil Rights Division, 950 Pennsylvania, Ave, NW, Washington, DC 20530, CRT.FOIArequests@usdoj.gov, 202-514-4210. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When seeking records about yourself from this system of records or any other CRT system of records, your request must conform with the Privacy Act regulations set forth in 28 CFR 16 Part D. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from CRT's Chief Privacy and Freedom of Information Act Officer (site/phone/email).

In addition, you should:

- Explain why you believe CRT would have information on you.
- Specify when you believe the records would have been created.
- Provide any other information that will help the FOIA staff determine how to search for the most responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records. Without the above information, CRT may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the “RECORD ACCESS PROCEDURES” paragraph, above. All requests to contest or amend records must be in writing and the envelope and letter 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. Some information may be exempt from the amendment provisions as described in the “EXEMPTIONS PROMULGATED FOR THE SYSTEM” paragraph, below. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

More information regarding the Department’s procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR §16.46, “Requests for Amendment or Correction of Records.”

NOTIFICATION PROCEDURES: Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the

same procedures as those identified in the “RECORD ACCESS PROCEDURES” paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

[FR Doc. 2026-08317 Filed: 4/28/2026 8:45 am; Publication Date: 4/29/2026]