Federal Government, or national security, resulting from a suspected or confirmed breach.

(o) To any agency, organization, or individual, such as the Government Accountability Office, a Federal Office of the Inspector General, or the Office of Special Counsel, for the purpose of performing authorized audit or oversight operations of DEA, including those related to fraud, waste, and abuse, and meeting related reporting requirements.

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

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored in electronic form. Electronic records are stored in databases and/or on hard disks, removable storage devices, or other electronic media with appropriate security and access limitations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records generally are retrieved by reference to an individual's name or personal identifier (*e.g.,* DEA number), by the relevant unit/location, or by reference to the equipment provided. Access requires two-factor authentication methods. Authorized users must have official authorized purpose(s) and appropriate access permissions.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system will be retained and disposed of in accordance with the appropriate records schedules approved by the National Archives and Records Administration (NARA) including, but not limited to, General Records Schedule (GRS) 4.1–010 Tracking and Control Records; GSR 5.4–010 Facility, Equipment, Vehicle, Property and Supply Administrative and Operational Records, and NARA-approved DEA schedules for Accountable Personal Property and Law Enforcement Officer Training Files.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information in this system of records is maintained in accordance with applicable laws, rules, and policies on protecting individual privacy. Specifically, information in this system of records is safeguarded in accordance with Department of Justice rules and policy governing automated systems security and access; and is protected by physical security methods, administrative processes, and technical means, including dissemination and access controls. These safeguards include all technical equipment in which information in this system of records is stored being maintained in restricted areas. For example, the servers storing electronic data and the backup tapes that are stored onsite are located in locked rooms with access limited to authorized agency personnel. Backup tapes stored offsite are maintained in accordance with a government contract that requires adherence to applicable laws, rules, and policies. Internet connections are protected by multiple firewalls. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations. Users of individual computers can only gain access to the data by a valid user identification and authentication. Access to individual computers requires two factor authentication.

RECORD ACCESS PROCEDURES:

All requests for access to records must be made in writing, in accordance with 28 CFR part 16, and may be submitted electronically by visiting the DEA FOIA Public Access Link Portal: *https://ifa.dea.gov/foia/,* or made via hard copy letter. If submitted via letter, inquiries should be addressed to: 'Drug Enforcement Administration, Attn: Freedom of Information and Privacy Act Section, 8701 Morrissette Drive, Springfield, Virginia 22152,' or addressed to the System Manager listed above with the envelope and letter clearly marked 'Privacy Access Request.' The request must include a general description of the records sought with sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request also must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury and dated. Although no specific form is required, you may obtain a DEA-specific form (*DEA–382 FOIA/PA Request Letter*) to make a 'Privacy Access Request' to DEA. The form is available on the Privacy Act page of the FOIA section of the *DEA.gov* website at *https://www.dea.gov/foia/foia-privacy-act.*

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR part 16 Subpart D, ''Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974.''

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend information maintained in the system must direct their request according to 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.is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

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. Hard copy inquiries should be addressed to: Drug Enforcement Administration, Attn: Freedom of Information and Privacy Act Section, 8701 Morrissette Drive, Springfield, Virginia 22152; or an electronic request may be filed at the DEA FOIA Public Access Link Portal: *https://ifa.dea.gov/foia/.*

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2026–08318 Filed 4–28–26; 8:45 am]

BILLING CODE 4410–09–P

DEPARTMENT OF JUSTICE

[Docket No. OLP184]

Notice of Requests for Certification of Capital Counsel Mechanisms of Florida and Mississippi

AGENCY: Department of Justice.

ACTION: Notice.

SUMMARY: This notice advises the public that the States of Florida and Mississippi have requested certification of their capital counsel mechanisms by the Attorney General and that public comments may be submitted to the Department of Justice regarding these requests.

DATES: Written and electronic comments must be submitted on or before June 29, 2026. Comments received by mail will be considered timely if they are postmarked on or before that date. The electronic Federal Docket Management System (FDMS) will accept comments until Midnight Eastern Time at the end of that day.

ADDRESSES: Please reference ''Docket No. OLP184'' on all electronic and written correspondence. The Department encourages all comments to be submitted electronically through *http://www.regulations.gov* using the electronic form provided on that site. Paper comments that duplicate the electronic submission should not be submitted. Individuals who wish to submit written comments may send those to the contact listed in the **FOR FURTHER INFORMATION** section immediately below.

FOR FURTHER INFORMATION CONTACT: Aaron Haviland, Counsel, Office of Legal Policy, U.S. Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530; telephone (202) 514–4601.

SUPPLEMENTARY INFORMATION: Chapter 154 of title 28, United States Code, provides special procedures for federal habeas corpus review of cases brought by indigent prisoners in state custody who are subject to capital sentences. These procedures may be available to a State only if the Attorney General of the United States has certified that the State has established a qualifying mechanism for the appointment, compensation, and payment of reasonable litigation expenses of competent counsel. 28 U.S.C. 2261, 2265; 28 CFR part 26.

This notice advises the public, pursuant to 28 CFR 26.23(b), that the States of Florida and Mississippi have requested certification of their capital counsel mechanisms by the Attorney General. Public comment is solicited regarding these requests. The requests and supporting materials may be viewed at *https://www.justice.gov/olp/pending-requests-final-decisions*.

Dated: April 21, 2026.

Daniel E. Burrows,

Assistant Attorney General, Office of Legal Policy.

[FR Doc. 2026–08319 Filed 4–28–26; 8:45 am]

BILLING CODE 4410–BB–P

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 May 29, 2026.

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 email, 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