Privacy Impact Assessment
for
Legal Files

September 24, 2025

Gregory Jones

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

Legal Files has been configured and implemented in several divisions of the CFTC. The Division of Enforcement (DOE) Office of Chief Counsel (OCC), Office of General Counsel (OGC) e-Discovery, OGC Employment and Labor, OGC General Law, OGC Litigation, Office of Proceedings, Secretariat, and OGC Ethics use Legal Files to manage matters and all related documents, activities, and correspondence for purposes of organization, litigation, and reporting. Additionally, Legal Files enables relationship management, calendaring, document assembly, time and expense handling, e-mail, and workflow. Each area is assigned to a configured site so that the data can be separated or accessible for users as necessary. Legal Files is supported on the front-end by Litigation Support Specialists and Subject Matter Experts, and on the back-end, including upgrades, by the Subject Matter Experts.

Legal Files is centralized and configurable by group or site to track, manage, and report on custom fields, involved persons in the matters, incoming and outgoing documents, and calendar and task data. It has a document assembly tool that leverages the data within the system to generate related documents from matters. Legal Files also has a query and reporting capability which allows groups to provide reports on all facets of the cases or matters Commission-wide.

Legal Files has an integration with the CFTC.gov portal, where consumers can submit a Tip Complaint Referral (TCR) a Whistleblower Tip Complaint Referral (WB TCR) or an Office of Proceedings Complaint. Selected information that the consumer fills out on the portal screens, along with up to ten attachments, are routed to a Legal Files server, where the service picks up the files and creates a matter and fills out certain fields in Legal Files. A notification is then sent to selected users to notify them of the new matter being created. Each office has different data elements and screens that have been created by the eLaw team in the Division of Administration in Information Technology branch to accommodate their business needs.

CFTC users access the application via an internal website accessible when connected to the CFTC network. Data is stored in a structured query language (SQL) database and on dedicated file servers for documents created by Microsoft 365 (M365), Microsoft Office, and Adobe Acrobat applications.

1. AUTHORITIES AND OTHER REQUIREMENTS

1.1 What legal authority(ies) permit or require the CFTC to collect, use, maintain, or disseminate the information in the system, project, or program?

The Commodity Exchange Act, 7 U.S.C. § 1 et seq., and the rules and regulations promulgated thereunder, establishes the CFTC and provides the authority for the CFTC's regulatory, enforcement, and market oversight activities as well as the authority for general operations of the CFTC, all of which may lead to the collection, maintenance, use, and dissemination of information in Legal Files. In addition, the Administrative Procedure Act, 5 U.S.C. §§ 551-559, Federal Rules of Civil Procedure, and state and federal statutes and case law govern the preservation, collection, and production of information in connection with regulatory activities, actual or anticipated litigation, and responses to subpoenas, all of which may lead to the collection, maintenance, use, and dissemination of information in Legal Files.

1.2 Is there a Privacy Act System of Records Notice(s) (SORN(s)) that applies to the information in the system, project, or program? If yes, please identify it. If no, please explain why not.

Yes. The CFTC-3, Docket Files for Reparations and Administrative Adjudication, CFTC-10, Investigatory Records, CFTC-16, Enforcement Case Files, CFTC-17, Litigation Files – OGC, CFTC-29, Reparations Cases Closed in the Complaints Section, and CFTC-49, Whistleblower Records, SORNs may apply to certain records in Legal Files. The CFTC's SORNs are available at CFTC.gov/privacy.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system is hosted by a Cloud Service Provider (CSP), please identify the CSP and state whether the system has Federal Risk and Authorization Management Program (FedRAMP) authorization.

The applicable accreditation boundary is Legal Technology Services – Legal Files, which was issued an ATO issued on May 22, 2023, and placed into continuous monitoring.

1.4 Is there a records retention schedule(s) approved by the National Archives and Records Administration (NARA) that governs the retention of the records maintained in the system, project, or program? If yes, please identify the schedule. If not, please explain.

Yes. The records in Legal Files vary in type and are subject to different retention schedules. These include General Records Schedule (GRS) 4.2, Item 020, Access and disclosure request files (DAA-GRS-2016-0002-0001) and GRS 6.1. They also include CFTC Mission Schedules 301, Legal Representation and Advice (DAA-0180-2018-0006-0003); 401, Customer and Official Inquiry Files (DAA-0180-2012-0003-0001); 402, Investigations Closed without Litigation (DAA-0180-2012-0003-0003); 403, Enforcement Case Files (DAA-0180-2012-0003-0006); 404, Closed Matter Summaries (DAA-0180-2021-0002-0001); 405, Whistleblower Submission Files

(N1.180.12.2); 407, Non-records from Record Codes 401, 402, and 403 (CFTC Filing Instruction); 411, Docket Files - Cases filed from October 2010 to present, Permanent records in each docket file (DAA-0180-2013-0005-0004); 412, All other Docket Files - Cases filed from October 2010 to present, All other Records (DM-0180-2013-0005-0005); 414, Docket File Tracking Systems (DAA-0180-2015-0001-0003); 423, Administrative Wage Garnishment Case Files (DAA-0180-2015-0001-0004); and 431, Landmark Inquiries, audits, investigations, litigations and similar events (DAA-0180-2021-0001-0001).

1.5 Please list all forms or other information collection instruments that are used to collect the information in the system. If the information collected is subject to the Paperwork Reduction Act, provide the name of the form or information collection and the applicable OMB control number.

The forms used in collecting information that enters Legal Files include "Form TCR Tip, Complaint or Referral" (OMB Control Number 3038-0082), "CFTC Reparations Complaint form" (CFTC Form 30, OMB Control Number 3038-0115), and "FORM TCR TIP, COMPLAINT OR REFERRAL" (electronic, https://forms.cftc.gov/Forms/TCR).

2. INFORMATION

2.1 Identify the information that the system, project, or program collects, maintains, uses, or disseminates.

The information that Legal Files collects, maintains, and disseminated is wide-ranging due to the various divisions and offices within the CFTC that make use of the system. The PII for the parties can be submitted by the party or updated by CFTC staff. Elements of PII in Legal Files may contain personal and financial identifying numbers (e.g., Social Security number, driver's license number, and employee ID) biographical and appearance information (e.g., name, date of birth, citizenship, height, weight, and race), contact and employment information (e.g., phone number, email, address, and employer).

2.2 Is the information collected directly from the individual and, if not, what are the sources of information collected. How is the information obtained?

The public can submit PII to CFTC via physical mail, phone, and email for manual entry by CFTC staff into Legal Files. Also, members of the public as complaining parties in matters can submit forms with PII using the CFTC.gov Whistleblower Complaint Form or Securities and Exchange Commission Form TCR, Tip, Complaint or Referral. Alternatively for Proceedings, PII is submitted by the complaining party

through the submission of the electronic (at CFTC.gov) and physical Reparations Complaint form (Form 30). PII involved in all Division operations can be input manually.

2.3 What steps are taken to minimize the collection of information in the system, project, or program?

Given the general investigative nature of the information contained in Legal Files, generally steps are not taken to minimize the collection of data in the system. It is not always clear at the outset what information will be relevant to a particular matter and Legal Files ingests voluminous quantities of information and records in order to manage and track it, and to enable analysis.

2.4 Discuss how the accuracy, integrity, and/or quality of the information identified above are determined.

At present, there is not a process for determining the accuracy, integrity, and/or quality of the information. PII is submitted by complaining parties and defendants, and can be updated by each office, such as DOE and Proceedings. There is no formal policy to do so. PII can be entered by other offices/divisions, but to the extent that they want to validate or update the PII is up to them.

2.5 Privacy Impact Analysis: Related to the Collection and Characterization of the Information

There is a risk that information will be unnecessarily collected and maintained in Legal Files or that it will be inaccurate. Legal Files processes information received for analysis from CFTC systems of records. There are detailed procedures in place to ensure that information that enters the analytic cycle is limited to only that which is necessary. While at present, there are no measures in place to ensure accuracy, all the data in Legal Files is owned by other Divisions and CFTC groups. It is CFTC attorneys who request and receive information that enters Legal Files, and therefore strict procedural norms and laws are in place and are observed. As a result, risk related to accuracy, quality, and integrity is minimal.

3. USE OF THE INFORMATION

3.1 Describe how the information is used internally at the CFTC to support a business purpose.

Information in Legal Files is used to manage matters, files, and cases to support office and division needs carrying out the CFTC's administrative, regulatory, and

enforcement roles. Further, a query and reporting capability allows groups to provide reports on all facets of the cases or matters Commission-wide.

3.2 Identify all programs or offices, and an approximate number of individuals, within the CFTC that have assigned roles and responsibilities with respect to the system, project, or program or with whom information is shared. Explain how each uses the information.

The CFTC restricts access to Legal Files to those employees and contractors who have a need to know the information to perform their job duties. In total approximately 300 CFTC employees and contractors from the Division of Enforcement, and the Office of the General Counsel use Legal Files to house information related to matters. In addition to the federal employees serving in those areas, contract employees use Legal Files to provide both mission-specific and technical system support.

3.3 Privacy Impact Analysis: Related to the Internal Access and Use

There is a risk that the information maintained in Legal Files will be accessed by an unauthorized individual or accessed by an authorized individual for an unauthorized purpose. These risks are mitigated through the use of role-based access controls including user provisioning, permissions management, and access controls. User access is also mapped to organizational duties performed to ensure that users are only processing data specific to their authorized functions. Additionally, all individuals who have assigned roles and responsibilities within Legal Files agree to CFTC Rules as a condition for access.

4. INFORMATION SHARING

4.1 Is the information shared outside of the CFTC as part of usual agency operations? If so, identify the organizations or individuals with whom the information is shared, how and *why* it is shared, and how it is to be used.

As a part of the ongoing investigation and litigation of matters, the DOE may share Legal Files data with third parties outside of the CFTC who are a party or involved in the matter. CFTC attorneys may approve the sharing of data via secure transmission with opposing counsel or other government agencies to comply with disclosure requirements related to litigation matters. On the whole, information is shared in usual Commission operations that are part of adjudications, investigations, enforcement, litigation, and reparations. Sharing outside of CFTC is done via postal mail or other secure delivery services, secure email, secure file transfer protocol, or on external media.

4.2 How is the information sharing described in 4.1 compatible with the purpose for which it was originally collected described in 3.1?

The sharing described above is done to achieve the purposes described in 3.1 and/or, consistent with the SORNs applicable to the records being disclosed. All disclosures of records that are covered by the Privacy Act are consistent with applicable routine uses in the relevant SORNs. For example, blanket routine use 2. Permits sharing with the Department of Justice, the Securities and Exchange Commission, the United States Postal Service, the Internal Revenue Service, the Department of Agriculture, the Office of Personnel Management, and to other Federal, State, local, territorial or Tribal law enforcement or regulatory agencies for use in meeting their statutory and regulatory requirements; blanket routine use 13. permits sharing with personnel performing or working on a contract, service, grant, cooperative agreement, or job for the Federal government; and blanket routine use 15. permits sharing with the Department of justice or in a proceeding before a court, adjudicative body, or other administrative body which the agency is authorized to appear, when CFTC is involved and the information is relevant and necessary to the litigation.

4.3 Is the information sharing documented in a Memorandum of Understanding, other information sharing agreement, or a contract?

Contractor access to Legal Files is subject to a contract with the CFTC. Information sharing with other agencies is permitted by 7 U.S.C. §§ 12 and 16 by access agreements executed under authority delegated to the Director of Enforcement. Other sharing in the context of litigation is done pursuant to requirements and restrictions in law and regulation.

4.4 Are there limitations on re-dissemination of the information by the third party in place, either in the documents identified in 4.2 or otherwise?

The contract limits the use of the information accessed by contractor staff to only that which is necessary to meet the requirements of the contract. The cooperative access agreements entered into with other agencies govern the appropriate use of the information provided and when information is disclosed in the context of litigation, there may be a protective order restricting further use and dissemination of the information. In other instances, such as when information is provided pursuant to the FOIA or the Privacy Act, there is no restriction on what the recipient may do with that information though it would have been redacted as permitted or required by applicable law. It is similar for other disclosures.

4.5 Describe how the system, project, or program accounts for and maintains a record of disclosures outside of the CFTC.

An accurate accounting of disclosures is not a fully implemented process for Legal Files. The manual process is documented through an Access Request where requests for information are documented. Once the CFTC provides an individual with an Access Grant, the access request and grant are stored within Legal Files and detail the name and address of the person or agency to which a disclosure is to be made. Currently, Legal Files does not document the date the data was shared or the description of the data that was shared to the requestor from Legal Files. For records subject to the Privacy Act, there is an internal tracking system that is utilized to comply with the requirement for retaining an accounting of disclosures. The internal tracking system is a ticketing system that tracks the date of the request for information, date the information is sent to the third-party, nature, and name of third-party to which the disclosure was made.

4.6 Privacy Impact Analysis: Related to Information Sharing

There is a risk that information in the system will be disclosed outside of the CFTC for a purpose that is not consistent with the purpose for which it was collected and/or that once shared it will be further disseminated for an unintended purpose. This risk is mitigated by sharing information only in accordance with the applicable SORNs and/or, where the records shared are not covered by the Privacy Act, consistent with applicable laws and regulations; and by establishing language in contracts and information sharing agreements that clearly defines appropriate use of the information.

5. DATA RETENTION

5.1 Explain how long and for what reason the information is retained.

Information in Legal Files is retained in accordance with applicable retention schedules identified in Section 1, which vary in accordance with the type of information. Records are archived, deleted, or destroyed in accordance with an archiving standard operating procedure (SOP) for information in Legal Files. Due to the varied nature of the records in Legal Files, retention timelines vary significantly. For example, investigations closed without litigation, enforcement case files, and non-records are transferred to off-site storage or destroyed 30 days after last related actions, appeal, or matter or case closure. Some records like docket files, administrative wage garnishment case files, access and disclosure request files, are generally maintained for 3 years. Customer and official inquiry files and legal representation and advice records are retained for 5 and 10 years, respectively. Some records are maintained for a mid-range of 15 years such as landmark inquiries, audits, and investigations and whistleblower submissions. Closed matter

summary records are maintained 50 years after matters are closed, and docket file tracking systems records are maintained until they are no longer needed for business.

The records are maintained and then disposed of in accordance with records disposition schedules for the records involved, as approved by and per the applicable records schedule. When information is subject to a litigation hold, the normal retention period is suspended during the hold. When the litigation hold ends, the normal retention schedule applies, and the CFTC works to dispose of information according to the schedule.

5.2 Describe how the information is disposed of at the end of its retention period.

Once records in Legal Files have reached the end of their retention period and are approved for disposal, CFTC staff or contractors under the supervision of CFTC staff permanently dispose of the related information. Records are deleted in accordance with the CFTC Records Management Manual and using the Records Destruction Approval Form. On an ad hoc basis in accordance with an SOP, closed matters are identified for archiving in accordance with approved records schedules.

5.3 Privacy Impact Analysis: Related to Retention

There is risk that information in Legal Files may be kept longer than is necessary to meet the business need for which it was collected. This risk is mitigated by destroying and deleting source records in accordance with the applicable retention schedule. Risk is partially mitigated by having an SOP in place.

6. NOTICE

6.1 How are individuals provided notice prior to the collection of their information? If they are not provided notice, please explain why.

Legal Files does not collect information directly from individuals and, therefore, does not provide notice directly to individuals. The information in Legal Files is obtained from CFTC.gov and via manual upload of information by CFTC staff. Where required, notice is provided to individuals at the point of the original collection of information, prior to ingestion into Legal Files via, for example Privacy Act statement on forms such as the Whistleblower Tip and Complaint form and the Reparations Complaint form. Notice is also provided to the public about what information the CFTC collects and for what purposes via publication of the SORNs identified in Section 1.2 and through publication of this PIA.

6.2 Do individuals have the opportunity to consent to the use of their information or decline to provide their information? Please explain.

Individuals do not interact directly with Legal Files and do not have the opportunity to consent to the inclusion of their information in the system.

6.3 Privacy Impact Analysis: Related to Notice

There is risk that individuals may not receive adequate notice concerning why their information is being collected and how it will be used. This risk is mitigated via Privacy Act statements on the relevant forms, publication of this PIA, through publication of the applicable SORNS, and via the provision of information on cftc.gov. Given the nature of some of the records collected in Legal Files, it may not be feasible or required to provide notice to individuals about the collection and use of their information.

7. REDRESS

7.1 What procedures are in place that allow individuals to access their information?

Certain records contained in Legal Files are included in Privacy Act systems of records that have been exempted from the access provisions of the Privacy Act. Individuals may request access to non-exempted records by following the procedures outlined in the relevant SORNs and the Commission's regulations at 17 C.F.R. Part 146.

7.2 What procedures are in place to allow individuals to correct inaccurate or irrelevant information about themselves?

CFTC staff members are responsible for manual corrections to information about them as system users. Members of the public have no access to the Legal Files system itself, and certain records within Legal Files may be exempted from the amendment provisions of the Privacy Act. Individuals may request amendment of non-exempted records by following the procedures outlined in the relevant SORNs and the Commission's regulations at 17 C.F.R. Part 146.

7.3 How are individuals notified about the procedures for correcting their information?

The procedure for submitting a request to correct Privacy Act covered information is outlined in the applicable SORN and/or in the Commission's regulations at 17 CFR Part 146.

7.4 Privacy Impact Analysis: Related to Redress

There is a risk that individuals will not be able to access information about themselves that is contained in the system nor be afforded an opportunity to correct that information. This risk is mitigated by providing individuals, where required and appropriate, with information about how to access and request amendment of their records through the instructions provided in the applicable SORNs and relevant Commission regulations.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

CFTF employs a variety of physical, technical, and administrative controls to secure Legal Files. Information within Legal Files is generally only accessible within the CFTC environment using CFTC-issued equipment. Access is limited by user role and "need-to-know." Further, multiple layers of approval are required for CFTC personnel to be granted access, personnel are required to follow CFTC Rules of Behavior, and annual security and privacy awareness training are required.

8.2 Are audit logs generated reflecting access and use of the information in the system? If not, please explain. If so, please describe how often they are reviewed and for what purpose.

Legal Files has robust audit logs that contain information regarding login/logout, records viewed, records edited, and document downloads. Logs themselves include very limited PII such as username, case name, case/matter ID, record creators/modifiers. Audit logs are created continuously, whenever an action for a matter is taken, and are reviewed as needed to troubleshoot any user and system anomalies.

8.3. What procedures are in place to determine who has access to the system, and are they documented?

Each CFTC practice area, Division, or Office has a Business Management Unit (BMU) which determines role-based access needs. CFTC staff members route access requests through supervisors, managers, and BMU into Service Now. Requests for access are made via Service Now and Legal Files subject matter experts create user accounts for the corresponding Division with the appropriate access controls in place.

8.4 Describe what privacy training is provided to users, either general or specific to this system or project.

All CFTC staff and contractors are required to complete Cybersecurity and Privacy Awareness Training prior to gaining access to the CFTC network and annually thereafter. Users who do not complete the annual training lose their access.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

There is a risk that the system is not audited and that the Commission is not accountable concerning the collection, maintenance, and use of the information in the system. This risk is mitigated because audit logs are generated and a Privacy Impact Assessment is available for review as needed. It is further mitigated because the BMU must request and receive access through Service Now for user account creation. Additionally, all users who access the system receive annual training and are required to sign rules of behavior.