Privacy Impact Assessment
for
NetDocuments Document Management System (NetDocuments)

March 2025

Point of Contact
Chris Kirkpatrick
Office of the General Counsel/
Secretariat and Information Management Branch

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

The Secretariat Electronic Document and Content Management System procured from NetDocuments and known as Document Management System (NetDocuments) is a cloud-based, Software-as-a-Service (SaaS) solution for the management of the Commission's Central Files. The Central Files, for which the Secretariat is the custodian, are the permanent records of all official actions by and related submissions to the Commission. NetDocuments is intended to provide an integrated platform for managing the documents in the Central Files throughout their lifecycle, including intake processing upon receipt from external or internal sources, indexing of records with metadata, maintenance and storage in a secure repository, search and retrieval for future use, and disposition by transfer to the National Archives and Records Administration (NARA).

The business owner of NetDocuments is the Secretariat Section of the Secretariat and Information Management Branch of the Office of the General Counsel.

The records maintained in the Central Files result from or are required to document the activities of the Commission and its operating Divisions and supporting Offices carried out under the authority of the Commodity Exchange Act (CEA).

In general, the information about individuals that is collected, used, maintained, or disseminated by NetDocuments may include the following types of information from members of the public: regulatory compliance, law enforcement, and whistleblower information; public affairs information; and personal identity and authentication information. NetDocuments also collects, uses, maintains, or disseminates the following types of information regarding CFTC employees and contractors: human resources, workforce management, security management, and planning/budgeting information; public affairs information; and personal identity and authentication information.

NetDocuments will be used exclusively within the CFTC by Secretariat employees and contractors. CFTC employees and contractors from the Division of Administration – IT Branch and the Division of Data – Portal Team may be involved with NetDocuments for maintenance and technical support purposes.

NetDocuments receives documents and information from three sources: (a) The Secretariat generates paper and electronic documents, or receives such documents via physical delivery or email, that are then manually uploaded to NetDocuments;

(b) For certain manually-uploaded documents resulting from business processes tracked in CFTC's Legal Files information system, process information associated with those documents is automatically sent from Legal Files to NetDocuments; and (c) Members of the public submit certain forms and other information through the CFTC Portal, which is a front-end information collection mechanism supporting both anonymous users, who generally submit completed CFTC forms such as whistleblower reports, and registered users, who provide diverse formats of business information supporting CFTC's mission. These submissions are captured in the Secretariat's records as filings with the Commission. The documents and/or information in each submission are automatically sent to NetDocuments.

The Secretariat may provide information from NetDocuments to other CFTC Offices and Divisions when those offices submit requests to the Secretariat for documents maintained within NetDocuments. The Secretariat locates the requested document(s) within NetDocuments and sends a copy to the requesting Office or Division. Once an Office receives a copy of a document or documents in NetDocuments, any external sharing or other handling of that copy is determined and executed by the requesting Office or Division, and the Secretariat neither authorizes nor controls such incidences of external sharing.

When records in NetDocuments reach the end of the timeframe for CFTC custody specified in the applicable records schedule, the Secretariat sends documents and their associated metadata from NetDocuments directly to the NARA.

Certain information stored in NetDocuments may contain sensitive personally identifiable information (PII), such as identifying numbers, contact information, biographical information, and signatures. Such PII may appear in a variety of contexts, including law enforcement, regulatory compliance, whistleblower, human resources, security management, workforce management, public affairs, planning and budgeting, and personal identity/authentication information. Sensitive information in NetDocuments will be safeguarded and risk to individuals mitigated through technical controls applied to the NetDocuments application and the CFTC IT environment where it interfaces with NetDocuments, as well as administrative controls limiting who is authorized and enabled to access and use this information system.

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?

NetDocuments' collection, use, maintenance, and sharing of information is authorized by the Commodity Exchange Act, 7 U.S.C. 1 et seq., and the rules and regulations promulgated thereunder.

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.

The following SORNs may apply to records in NetDocuments:

- CFTC-1, Enforcement Matter Register and Matter Indices (Exempted);
- CFTC-2, Commission Correspondence Files;
- CFTC-3, Docket Files for Reparations and Administrative Adjudication;
- CFTC-10, Investigatory Records (Exempted);
- CFTC-13, Interpretive, Exemptive, and No-Action Files;
- CFTC-16, Enforcement Case Files;
- CFTC-17, Litigation Files-OGC;
- CFTC-41, Requests for Confidential Treatment;
- CFTC-49, Whistleblower Records (Exempted); and
- CFTC-58, Advisory Committees.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system, or involved project or program, 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.

NetDocuments is located within the vendor NetDocuments' environment within the Azure cloud and is FedRAMP® approved. The CFTC issued an ATO for NetDocuments in August 2024.

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 NetDocuments are subject to the CFTC-specific Records Schedule 303, *Official Communications, Actions, Decisions, and Guidance,* DAA-

0180-2018-0006-0001. These are permanent records and are transferred to NARA after 30 years.

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.

While copies of certain CFTC Portal forms are sent to NetDocuments upon submission via the Portal to the CFTC by members of the public, no forms are used to collect information or documents for NetDocuments. NetDocuments collection is not subject to the Paperwork Reduction Act.

2. INFORMATION

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

NetDocuments contains the following PII data elements about CFTC employees whose information is contained in documents maintained in NetDocuments:

- Names
- Business contact information
- State Bar numbers
- Signatures

NetDocuments contains the following PII about members of the public whose information is contained in documents maintained by NetDocuments:

- File/Case ID Number
- Legal Entity Identifier
- State Bar number
- National Futures Association ID
- Business phone number, email address, mailing address, fax number
- Name
- Group/Organization membership
- Resume or curriculum vitae
- Employment information
- Signatures

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?

No, NetDocuments does not collect any information directly from individuals. NetDocuments collects information in the following three manners:

1. The Secretariat generates paper and electronic documents, or receives such documents via physical delivery or email from inside and outside of CFTC, that are then manually uploaded to NetDocuments;

2. For documents resulting from business processes tracked in CFTC's Legal Files information system, which consist of completed seriatim voting packages, completed absent objection review packages, informational memoranda, and congressional correspondence, process information associated with those documents is automatically sent from Legal Files to NetDocuments; and

3. For certain CFTC Portal submissions that are captured in the Secretariat's records as filings with the Commission, including but not limited to DCM Regulatory Oversight Committee Annual Report, Application for Registration, Swap Submission, Foreign Board of Trade (FBOT) Linked Contract Changes or Events, Swap Deposit Repository (SDR) Chief Compliance Officer (CCO) Annual Compliance Report (ACR), and Swap Execution Facility (SEF) Registration and Post-Registration Form SEF Exhibits, the documents in each submission and selected information from the completed CFTC Portal form entered by members of the public for that submission are automatically sent to NetDocuments.

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

No steps are taken to minimize the collection of information, including PII, by NetDocuments. The information in this system is intended for documentary and archival purposes, capturing the status quo of a submission or decision as of the date the information is put into the system. Allowing individuals to limit the collection, use, maintenance, or sharing of their PII would undermine the purpose of this system.

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

No steps are taken to determine the accuracy, integrity, or quality of the information, including PII, collected by NetDocuments. The information in this system is intended for documentary and archival purposes, capturing the status quo of a submission or decision as of the date the information is put into the system. Allowing any editing or amendment of the captured information, whether for purposes of accuracy, integrity, or quality of the information or otherwise, would undermine the purpose of this system.

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

NetDocuments is not the original point of collection of any information it contains and relies on other sources of information for the documents and records, including PII, it collects. NetDocuments does not seek to limit the amount or type of PII collected or verify the accuracy of or correct any records it receives because to do so would undermine its primary purpose: to serve as a repository of past decisions and actions for reference and use for future actions and decisions. For documents manually uploaded by the Secretariat to NetDocuments, there is a risk that the information may not properly upload and potentially omit information in the target record. For such circumstances, the Secretariat reviews what was manually uploaded and if the uploaded file is not an accurate copy of the record as provided to the Secretariat via email or mail, the incorrect/inaccurate copy will be deleted from NetDocuments, and the record would then be reuploaded to ensure it accurately and fully represents the records at issue. Accordingly, the risk associated with collection and characterization of information in NetDocuments is low.

3. USE OF THE INFORMATION

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

The information in the system documents and maintains a permanent record of the official actions, decisions, policies, procedures, and communications to and from the Commission that impact the CFTC, registered entities and intermediaries, and potential Whistleblowers.

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 only individuals who have roles or responsibilities with respect to the system are the Secretariat staff, its contractors, and DA-IT developers and helpdesk staff. Approximately 10 total Secretariat staff users will access the system on a regular basis. The DA-IT developers or helpdesk will only access the system to troubleshoot if there are issues with connectivity of data flowing into the system. DA-IT is expected to have a "service account" which allows for automation to write data into NetDocuments.

The information contained in the collected decisions and filings are important to internal and external parties. The Secretariat accordingly receives many requests from all offices within the CFTC for this archival information and shares it internally with those offices upon request for business purposes such as seeing what the Commission has decided on similar issues in the past and reviewing previous filings from regulated entities to see what happened in those situations. Additionally, external parties seek this information through FOIA requests, and information in NetDocuments is provided to the FOIA team to respond, as appropriate, to those requests. The data must be downloaded from the system and sent to them by Secretariat staff. Other than the Secretariat and DA-IT, no other CFTC staff will have direct access to the system.

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

Access to records collected by NetDocuments is limited to those with an official need to know but is potentially available to any CFTC staff member. The Secretariat controls the process to access NetDocuments records. CFTC staff needing access to certain records in NetDocuments submit a request to the Secretariat including the official business need for the requested information and after confirming the official business need, the Secretariat staff searches for, finds, and sends a copy of the requested document(s) to the requesting CFTC staff member.

All activity in NetDocuments is monitored by its internal audit functionality and captured logging data is pushed to CFTC's instance of Sentinel in its Azure cloud environment. Based on the above, the risk associated with internal access and use is low.

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.

In the course of day-to-day business operations, information is shared outside of the CFTC from NetDocuments in only two instances. Appropriately cleared employees and contractors of the CFTC's NetDocuments vendor may have access to CFTC PII maintained by this information system when, e.g., responding to a CFTC request for technical assistance, pursuant to their contract with CFTC. Also, in accordance with the applicable retention schedule, the Secretariat will send NetDocuments records to the National Archives and Records Administration (NARA) for permanent recordkeeping.

Other than the above, no documents are directly shared from NetDocuments with an external person, agency, or other entity. Generally, other CFTC Offices or Divisions that request and receive copies of documents or records from this information system may decide to share that document with an external person, agency, or entity, in which case it will provide that document directly to the intended external person, agency, or entity. That Office or Division is responsible for such external sharing, and NetDocuments is neither involved nor notified.

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 external sharing related to the vendor's access to information in NetDocuments to respond to a CFTC request for technical assistance is necessary to maintain the records in the system and access them as needed. To the extent the records that the vendor accesses are covered by the Privacy Act, the relevant SORNs include a routine use that permits the disclosure to the vendor is covered by an appropriate routine use.

Likewise, the external sharing related to the Secretariat's sending of NetDocuments documents to NARA for permanent recordkeeping is compatible with the maintenance of these records as permanent records and is necessary to comply with applicable Federal Records requirements.

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

CFTC's Contract, with the vendor provides that the vendor's employees shall be provided access to CFTC information and information systems to the extent necessary to fulfill the Contract obligations, including the provision of HelpDesk support on an as-needed basis and available 24x7x365.

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 provides that the vendor agrees to use the information to which it has access only for the purposes of performing work under the Contract and to hold such information confidential. That provision further prohibits the vendor from directly or indirectly using or allowing the use of such information for any other purpose, and prohibits the vendor's employees from, either by direct action or by counsel, discussion, recommendation, or suggestion to any third party, reveal the nature or content of any confidential information without written authorization from the CFTC.

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

At the appropriate time, one of the two CFTC administrative users of the system will download copies of records to be sent to the NARA for permanent recordkeeping. To aid this process, the Records Management Unit (RMU) under the CFTC Secretariat and Information Management Branch maintains a spreadsheet of all documents, including NetDocuments records, that provides, in relevant part, a general description of the documents, the date the retention period expires, and the date the documents are sent to NARA. The RMU can identify which documents constitute NetDocuments records from the general description provided on the spreadsheet. Collectively, this always-available information can be used to create the accounting of disclosures even when the information is not recorded contemporaneous with the disclosure to NARA.

When a NetDocuments employee or contractor logs into NetDocuments and accordingly accesses CFTC's information, including PII, in response to an express request for technical assistance by one of the two CFTC administrative users of NetDocuments, the NetDocuments auditing function records all information regarding this access, including the time/date of the access, the identity of the person accessing the system/information therein, and the information accessed during that log-in session. The purpose of the access is not captured with the auditing function, however. To obtain that information, the Privacy Office will work with the CFTC administrative user requesting and authorizing the NetDocuments access of the information system and CFTC's information therein and, to the extent necessary, that administrative user will work with NetDocuments to obtain the requested information. Collectively, this always-available information can be used to create the accounting of disclosures even when the information is not recorded contemporaneous with the disclosure.

Notwithstanding, no information, documents, or other records are produced directly from NetDocuments to any persons or entities external to CFTC. As described above, other CFTC Offices and Divisions request copies of documents from

NetDocuments and, once provided to them from NetDocuments by the Secretariat, review them and decide whether, in the conduct of official business, the information, documents, or other records should be disclosed to external persons or entities. When disclosing such information externally, the CFTC Office or Division does not notify the Secretariat about that disclosure before or after making it. Accordingly, it is a practical impossibility for Secretariat to track any external disclosure of NetDocuments information, documents, or other records and that responsibility necessarily falls to the CFTC Office or Division making the external disclosure.

4.6 Privacy Impact Analysis: Related to Information Sharing

NetDocuments contains records that are intended for future use and reference by CFTC staff for internal and often external use. The only direct access to NetDocuments records from an external person or entity would be by personnel of the CFTC vendor in direct response to an express request for technical assistance from the CFTC administrator for NetDocuments. When such access is expressly granted, there is a risk that an individual could access CFTC PII that is unnecessary for the purpose of addressing the technical issue. To protect against that risk, the NetDocuments audit function tracks all activity, including any changes made to NetDocuments records/information. The other two avenues of externally sharing NetDocuments documents/records are indirect. When sending NetDocuments records to NARA for permanent record-keeping, the Secretariat downloads the documents from NetDocuments and then uploads those documents to a NARA portal. Other CFTC Divisions and Offices receiving NetDocuments documents in response to their express request made to the Secretariat can externally share those documents as determined by that Division or Office, which in most cases is done in the context of litigation or responses to Freedom of Information Act (FOIA) requests, where accuracy of the provided record vis a vis the original record is paramount not just to CFTC but to the ultimate recipient of the information. All such external sharing is done according to an already established routine use and in any event, the original copy of the shared record remains intact within NetDocuments. Accordingly, the risks associated with external sharing are low.

5. DATA RETENTION

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

The information contained within the system has been identified by NARA to be maintained indefinitely as permanent records due to the importance of the information contained within the documents. Pursuant to the applicable records schedule, the CFTC maintains the records for 30 years after which they transfer

custody to NARA. Before ultimate disposition and transfer to NARA, all NetDocuments records are used for reference and use in support of CFTC's mission.

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

When the CFTC transfers custody of these permanent records to NARA they will be batch-exported from the system and sent to NARA in whatever format (disk, hard drive, electronic file transfer, etc.) that NARA requires at the time of transmission.

NetDocuments does not track the date a document is to be sent to NARA. The CFTC administrator for NetDocuments will monitor the retention period of records and will create an Outlook calendar notice or other internal note, for the date when the document must be sent to NARA.

5.3 Privacy Impact Analysis: Related to Retention

All NetDocuments records are required to be permanently maintained pursuant to the applicable records schedule and a defined process is in place for transferring the records to NARA, by the Secretariat downloading those documents and then uploading them to the NARA online portal. No records are destroyed. The risk associated with retention is low.

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.

NetDocuments does not collect any documents or other information directly from individuals and accordingly does not provide notice to individuals upon the collection of their information. Individuals instead receive indirect notice of the collection of their data via the SORNs applicable to records in NetDocuments, which are identified in the response to Question 1.2 above, 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 have the opportunity to consent to the collection or any particular use of their PII by NetDocuments. To the extent there is an opportunity to consent or decline to provide PII to the CFTC for a particular purpose, that opportunity is presented to individuals at the original point of collection.

6.3 Privacy Impact Analysis: Related to Notice

Because NetDocuments does not collect any information directly from individuals, no notice is provided to individuals when NetDocuments collects their information. Any risk related to an individual not being provided with notice that their information is contained in NetDocuments is mitigated via publication of this PIA.

7. REDRESS

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

Individuals do not have access to NetDocuments to view information about themselves that may be contained therein. To the extent the information in NetDocuments is included in a Privacy Act system of records, individuals can submit a Privacy Act request by following the instructions in the applicable SORN and in 17 C.F.R. § 146.

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

Individuals do not have access to information about themselves in NetDocuments in order to make changes to or amend information about themselves. The information in this system is intended for documentary and archival purposes, capturing the status quo of a submission or decision as of the date the information is put into the system. Correcting or amending any PII collected could undermine the purpose of this system. Notwithstanding, if a document is impartially or mistakenly uploaded, the system administrator will delete the incomplete or unintended upload and, in the former case, will reupload the completed document. However, to the extent the information in NetDocuments is included in a Privacy Act system of records, individuals can submit a request for amendment by following the instructions in the applicable SORN and in 17 C.F.R. § 146.

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

Instructions concerning the procedure for correcting/amending information are set out in the SORNs identified in response to Question 1.2 and in 17 CFR § 146.8.

7.4 Privacy Impact Analysis: Related to Redress

As noted above, there is no process to correct or amend documents in NetDocuments because amending or correcting such information would undermine

this information system's intended purpose, which is to be an archive or reference source for Commission actions and other activities related and tangential to its mission. To the extent that documents in NetDocuments have incorrect or inaccurate information about an individual, that individual would need to seek an update or amendment from the original collection point/source for that information. Accordingly, the risk related to redress is low.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

NetDocuments and the information therein are secured with multiple layers of security including the following:

- Physical safeguards include onsite guards and ID badges;
- Administrative safeguards include access controls, the NetDocuments user manual, a contingency plan as part of the FedRAMP package, and the requirement to sign CFTC's Information Technology Rules of Behavior Acknowledgment form; and
- Technical controls include multifactor authentication (MFA) using a CFTC Personal Identity Verification (PIV), Federal Risk and Authorization Management Program (FedRAMP) certified data centers, and use of CFTC's Virtual Private Network (VPN).

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.

NetDocuments includes a Consolidated Activity Log that allows CFTC to see all interactions and access documents within CFTC's environment. This Log can be pulled/created at any time, but the scope of logged activity is limited to the 90 days immediately preceding the request for/creation of the Log. This Log includes names and Internet Protocol (IP) addresses. While the Consolidated Activity Log indicates what data sources are accessed and the activity involved with or changes to those data sources, they do not indicate how PII in NetDocuments is used. The Consolidated Activity Log collects data and send it in real time to Sentinel. There is no review of the Log before it is sent to Sentinel. CFTC's Enterprise Security Operations Center (eSOC) reviews Sentinel log data related to alerts received by eSOC and to alerts triggered by the source from which data in the logs are gathered. If any audit logs note suspicious activity, eSOC will follow the CFTC internal guidelines to address.

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

Only the two CFTC administrative users of NetDocuments will have the ability to request that users be added or deleted from the system. Upon an administrative user's request or approval, CFTC Division of Administration - Information Technology (DA-IT) staff will then add (or subtract) such individuals to (or from) the Active Directory (AD) to be able to log into NetDocuments through CFTC's Single Sign-On (SSO). Users must access the system through the CFTC network only. The two administrative users will only add other Secretariat users to the NetDocuments Active Directory who have roles and responsibilities in managing, maintaining, and updating the system and the data and information contained within it.

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

Completion of initial and thereafter annual security and privacy awareness training is a prerequisite to a user gaining and maintaining access to the CFTC network. All users must sign the CFTC Information Technology Rules of Behavior Acknowledgment, which memorializes this requirement. Access to the system is limited to those with an official need-to-know.

The requirement to complete security and privacy awareness training is immediately charged to an employee or contractor upon onboarding to CFTC, i.e., after their AD account is created, and must be completed within two days. If the training has not been completed in the two-day period, the user's AD account is automatically disabled, preventing that user from accessing the CFTC network to any degree, and the account remains disabled until the training has been completed.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Failure of an audit to detect potential malicious activity or improper access to NetDocuments Consolidated Activity Log risks the deletion or alteration of individuals' PII, which could negatively affect their access to the CFTC network and assets therein. An employee's or contractor's access to the CFTC network and assets therein is a condition of initiating and continuing engagement with CFTC. There is a low risk of stolen identity, because this information is business related and not personal, or of gaining access to the CFTC network, since more than a user's name and IP address information is required for access. These risks are mitigated by alerts set up by eSOC to identify any suspicious activity. Once the

alert is received, eSOC is notified and immediately responds and remediates any damage caused by the event.