Privacy Impact Assessment
for
Nexidia

September 24, 2025

Point of Contact
Gregory Jones

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

Nexidia is one in a suite of systems and tools that the CFTC's Division of Administration Information Technology Legal Technology (eLaw) operates and manages to enable CFTC legal professionals, generally in the Division of Enforcement, the Office of the General Counsel, and the Office of the Inspector General to quickly and accurately search, review, and categorize large volumes of audio and video files. It renders transcripts and enables CFTC personnel to generate and download notes about the content of the audio and video files.

Nexidia's review supports the management of audio and video data. In addition to allowing users to search large volumes of audio and video data with immediate results, it takes users easily to relevant sections of audio files responsive to search criteria. Microsoft Access formats metadata prior to loading into Nexidia. On the front end, Nexidia is supported by the CFTC Litigation Support Specialists, and on the back end it is supported by Electronic Document Discovery Specialists.

The audio and video files are generally obtained in the course of an investigation or litigation, often in response to a subpoena or 4G request, though there are other scenarios in which CFTC personnel would obtain audio and video files and employ Nexidia. The files are originally submitted to the CFTC's Central Processing Intake (CPI) team within the Litigation Support Branch who scan the files for viruses, prepare them for storage on the CFTC network, and load them into Relativity, another system that facilitates the review of electronic documents and files. All audio and video files in Relativity are moved from Relativity to Nexidia.

The CFTC legal professionals assigned to the particular matter in which the audio and video files were produced are then able to conduct in-depth and ad-hoc searches for spoken topics within the files on a greater scale and much more quickly than they would be able to do otherwise. Using Nexidia, they can locate content such as proper names, jargon, and specialized industry terms and they can also create searches using Boolean filters, metadata, and time and date parameters. The audio and video files contain personally identifiable information in the form of the audio and video recordings of the individuals present in the videos, as well as a potential variety of other PII that may be discussed in the audio and/or be present in the video files. The nature of the PII will vary considerably across different matters but could include biographic information, identifying numbers, and contact information.

The audio and video files in Nexidia, and the information that the CFTC legal professionals generate and extract via their searches and analysis, is used as appropriate in the context of the investigation or litigation, including, for example, by providing it to the other parties in litigation, to the relevant court or administrative body, and/or to other state and Federal agencies who may be collaborating on a particular matter.

Much of the information collected and processed in Nexidia is sensitive and confidential and is not generally releasable to the public. Given the nature of the information in Nexidia, access to the system is strictly limited to those who have a need-to-know, and those with system access are further limited to access only the matters to which they have been assigned. Nexidia also processes audio-video records when responding to FOIA and PA requests.

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 Nexidia. In addition, the Federal Rules of Civil Procedure and state and federal statutes and case law govern the preservation, collection, and production of information in connection with actual or anticipated litigation and responses to subpoenas, all of which may lead to the collection, maintenance, use, and dissemination of information in Nexidia.

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-10, Investigatory Records, CFTC-16, Enforcement Case Files, CFTC-17, Litigation Files – OGC, and CFTC-49, Whistleblower Records SORNs may apply to certain records in Nexidia. 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, 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.

The applicable accreditation boundary is Legal Technology Services - Nexidia, which was issued an ATO 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 Nexidia vary in type and are subject to various retention schedules. These 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.

Not applicable.

2. INFORMATION

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

The information in Nexidia consists of audio and video files that were obtained in the course of CFTC investigations and litigation as well as transcripts of those files generated within the system and any notes taken by the legal professionals responsible for reviewing them.

The information in Nexidia 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?

Information in Nexidia is generally not collected directly from the individual. Audio and video files that are submitted to the CFTC are loaded into Nexidia from Relativity. The audio and video files are generally collected by the Division of Enforcement via subpoenas and 4G requests and submitted to the CFTC's Central

Processing Intake (CPI) team within Litigation Support Services. CPI scans the files for viruses, prepares them for storage on the CFTC network, and loads them into Relativity, another system that facilitates the review of electronic documents and files. All audio and video files in Relativity are then moved to Nexidia.

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

Only audio and video files that are obtained in response to a subpoena or 4G request, or otherwise obtained or generated in the context of a CFTC matter, are loaded into Nexidia. Such requests for information are crafted to obtain information necessary for a particular investigation or litigation and once received they are loaded into Nexidia as is.

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

Audio and video files are loaded into Nexidia as received and no alterations are made to their content. In the course of an investigation and/or a case for litigation, the accuracy, integrity, and quality of the information is assessed by the relevant CFTC legal team. While it is possible that recordings can be fabricated or manipulated, sources are assumed to be providing accurate records of real events.

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

There is a risk that Nexidia will collect more information than is necessary to fulfill its business purpose and that the information will not be accurate. Case management and analysis identify and refine relevant information that is not filtered initially through input from Relativity. Targeted analysis is conducted respective to litigation requests which were designed to solicit information relevant to cases. While the risk of collecting more information than is necessary is not fully mitigated due to the nature and purpose of Nexidia, as described above, the protocols in place for taking in discovery responses in litigation or responding to same contribute to collecting only what is necessary in a particular instance do work to mitigate any over-collection. Likewise, the accuracy of the information is ensured to the greatest extent possible in context as described above.

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 Nexidia is used in the relevant investigation or litigation to develop and/or support the CFTC's analysis.

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.

DOE, OGC, and OIG users leverage Nexidia for in-depth ad-hoc searches for spoken topics across any amount of recorded content for investigative purposes. Users may download transcripts of the audio and video recordings within Nexidia. They can also take and download notes within Nexidia based off of the audio and video recordings.

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

There is a risk that the information maintained in Nexidia 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 Nexidia agree to CFTC Rules of Behavior 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, DOE may share data within Nexidia with third parties outside of the CFTC who are a party to or involved in the matter. DOE can also share data with other Federal and State agencies as a part of cooperative enforcement initiatives which facilitate the sharing of information in ongoing investigations and/or litigation. This information sharing is facilitated through the process of an access request and an access grant.

This includes information provided by individuals, firms, and other regulators for investigatory and enforcement purposes; information from forensic searches and collections pursuant to court order or discovery rules; and certain information from other CFTC systems, to include, for example, information needed for internal investigations or to respond to FOIA or Privacy Act requests or to requests from Congress.

Information in Nexidia may be shared outside of the CFTC with contractors who provide support to the system so that they can trouble shoot technical issues; with FOIA and other requesters when the information is responsive to a request and

releasable under applicable law; with opposing parties in litigation and to courts and other adjudicative bodies; and with other Federal and State agencies as a part of cooperative enforcement initiatives. 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, 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 an 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 Nexidia 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?

When information is disclosed in the context of litigation, there may be a protective order restricting further use and dissemination of the information. Information may be disclosed only to CFTC and contractor personnel directly concerned with the performance of the task order and who have a need to know such information to perform their assigned duties. It may be disclosed to no other parties, including CFTC and contractor personnel and any and all other non-CFTC parties, that do not have a need to know. In instances where access to Commission records is granted to other federal agencies or authorities, third party disclosure is prohibited, except in connection with an action or proceeding under the laws of the United States to

which the Commission, the United States, or that agency or authority is a party. When information is disclosed pursuant to the FOIA, there is no restriction on re-dissemination, but the information provided will have been appropriately redacted for public consumption. 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.

For instances in which Privacy Act covered information is disclosed externally to the CFTC, the litigation support branch records the date, nature, and purpose for sharing the information and the name and address of the entity or person to whom it will be disclosed.

4.6 Privacy Impact Analysis: Related to Information Sharing

There is some risk that records in the system may be disclosed outside of the CFTC for a purpose that is not consistent with the purpose for which it was collected. This risk is mitigated by confirming identities and contact information of collaborating external parties and carefully reviewing shared records to ensure that only required information is provided. There is also a risk that, once shared appropriately, records and information in the system will be used or shared further inconsistent with their original purpose. This risk is mitigated via CFTC rules of behavior and contract terms that limit the use of the information that the contractor can access to that which is necessary to achieve the terms of the contract.

5. DATA RETENTION

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

Information in Nexidia is retained in accordance with the 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 the archiving SOP. 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. Records like email and other electronic messages of capstone officials and permanent docket case files are transferred to NARA after 30 years. 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 CFTC records disposition 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 Nexidia 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. In most circumstances for information moving through Nexidia, matters reach closure status and access is removed. Then, data is archived. The information stored in file shares is backed up. Records are then retired to NARA facilities in accordance with prescribed schedules and any backups are destroyed. Records are deleted in accordance with the CFTC Records Management Manual and using the Records Destruction Approval Form. On a quarterly basis in accordance with an SOP, closed matters are identified for archiving in accordance with approved Division of Enforcement Records Schedule: 5 years for Leads, Preliminary Inquiries, and Investigations; 15 years for Litigations; and indefinitely for Permanent Records (matters identified as historical). At the end of retention periods, records are transferred to NARA.

5.3 Privacy Impact Analysis: Related to Retention

There is a risk that information in Nexidia may be kept longer than is necessary to meet the business need for which it was collected. This risk is mitigated by engaging in the manual review and deletion of records in accordance with applicable retention schedules.

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.

Nexidia does not collect information directly from individuals and, therefore, does not provide notice directly to individuals. Rather, Nexidia receives records and information from Relativity. Except in the cases of investigations or when information is provided by one individual that contains information about other individuals, appropriate notice is provided to individuals at the point of the original collection of information prior to ingestion into Nexidia. Notice is also provided to the public about what information is collected and for what purposes via publication of the SORNs identified in Section 1.2. Notice is also provided through 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 Nexidia 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. Where applicable, this risk is mitigated via Privacy Act statements at the point of collection from the individual and is also mitigated via publication of the applicable SORNs and as well as through publication of this PIA. Given the nature of the records collected for investigations and litigation, 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 Nexidia are included in Privacy Act systems of records that have been exempted from the access and amendment 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/amend inaccurate or irrelevant information about themselves?

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

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

The procedures for submitting a request to correct Privacy Act covered information are 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 or 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?

CFTC employs a variety of physical, technical, and administrative controls to secure Nexidia. Information within Nexidia 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 are required to complete annual security and privacy awareness training .

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.

Nexidia has audit logs that are created continuously, whenever an action in the system is taken, and that contain information regarding login/logout and audio and video records viewed and downloaded. Logs include very limited PII. Audit logs 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 Chief Trial Attorney (CTA) who determines role-based access needs. CFTC staff members route access requests through supervisors, managers, and CTA to the LSS. Then, the Electronic Document Discovery team processes the requests, grants access, and configures user functionality.

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

All CFTC employees and contractors are required to take Cybersecurity and Privacy Awareness Training prior to being provided access to the CFTC network, and annually thereafter. Any user who fails to meet the annual training requirement is subject to losing network 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 Electronic Document Discovery team has ultimate accountability for who has access to the system and at what level. Additionally, all users who access the system receive annual training and are required to sign rules of behavior.