U.S. Securities and Exchange Commission

Nexidia ESI Audio Searching Software
PRIVACY IMPACT ASSESSMENT (PIA)

October 9, 2014

Privacy Impact Assessment
Nexidia ESI Audio Searching Software v.10.1

General Information

1. Name of Project or System.
   Nexidia ESI Audio Searching Software v 10.1

2. Describe the project and its purpose or function in the SEC's IT environment.
   Enforcement receives audio recordings in many investigations. These are often recordings made by brokers of phone calls between broker representatives and customers. In a large case, there could be many hours (e.g. 5000 hours) of recordings. All of the recordings must be listened to in their entirety to locate sections of the recordings relevant to the investigation, if any. This often required allocating multiple staff or teams of interns and paralegals to complete the review in a timely fashion. Nexidia software allows the recordings to be loaded into a Microsoft SQL database and indexed. It also perform searches that dramatically improves the efficiency of the review process allowing staff to zero in on important conversations quickly. Instead of spending hundreds or thousands of hours listening to recordings, staff spend only minutes conducting online searches. The previous manual review increased the risk of missing important conversations and limited the number of hours of recordings that someone could listen to attentively. Due to the time consuming nature of manually reviewing audio recordings, staff were often reluctant to issue subpoenas for them.

3. Requested Operational Date? This system has been operational since 2011. A PIA was previously conducted and approved on 8/2/11. This PIA is being updated to ensure the current administrative and technical controls adequately protect the PII collected and any new privacy risks are mitigated.

4. System of Records Notice (SORN) number? SEC-42, Enforcement Files.

5. Is this an Exhibit 300 project or system? ☒ No ☐ Yes

6. What specific legal authorities, arrangements, and/or agreements allow the collection of this information? Title 15, United States Code, sections 77s, 77t, 78u, 77uuu, 80a-41, 80b-9, and 17 CFR 202.5.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   Digital audio recordings may contain an individual's name, address, telephone number, email address and other identifiers. The recordings may contain additional information regarding transactions between broker representatives and customers. In some situations, the recording system may also provide metadata about the recording, such as, phone numbers, time of call, and duration of call.

2. Does the project/system use or collect the social security number (SSN)? (This includes truncated SSNs)
   ☒ No.

☐ Yes. If yes, provide the function of the SSN and the legal authority to collect.

3. What are the sources of the data?
   Primary sources are individuals or entities responding to a subpoena request issued by the SEC in Enforcement investigations. For example, a brokerage firm may record phone calls between broker representatives and customers and provide the recordings as a part of their response to a subpoena.

4. Why is the data being collected?
   Data is being collected to expedite the review of many hours (e.g. 5000 hours) of recordings that Enforcement may receive in investigations. Previously it required the allocation of multiple staff in order to complete the review in a timely fashion. Nexidia dramatically improve the efficiency of the review process allowing staff to zero in on important conversations quickly. Nexidia audio searching allows staff to take advantage of an under utilized source of evidence and also reduce transcription costs in Enforcement investigations and litigation matters.

5. What technologies will be used to collect the data?
   Nexidia is a Commercial-Off-the-Shelf (COTS) software product that allows audio recordings received from external parties to be loaded into a database and indexed. The indexed data can then be exported from the database and used as a source of evidence in cases or litigation.

SECTION II - Attributes of the Data (use and accuracy)

1. Describe the uses of the data.
   Users access the system to perform searches or apply queries looking for phonetic matches for the search query. Analysis reports are presented to the user through a web interface. From within those analysis results, additional forensic searching may be performed on the resultant set of media. Enforcement staff will use data obtained from audio recordings in investigations and litigation.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern? ☒ No ☐ Yes If yes, please explain:

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   Data derived from the audio search system will be used in testimony and in litigation. The data is validated against other information obtained as part of the investigation to ensure data obtained is sufficiently reliable for making accurate and logical interpretations and judgements in litigation matters.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s): Data is shared with the following internal systems: Concordance (Litigation Support) and CaseMap. Concordance stores electronic

evidentiary documents, to include audio files, for Enforcement cases. Nexida has read/write capabilities to Concordance. It also allows investigative staff to link to audio recordings in the Case-Map databases where other evidentiary documents are linked. This allows all important pieces of evidence to be reviewed and tracked in one location.

2. Will the data be shared with any external organizations?
   ☒ No ☒ Yes If yes, please list organizations(s): Data may be disclosed in accordance with the routine uses found in SEC SORN SEC-42, Enforcment Files. Additionally, data may be shared with other law enforcement agencies or opposing counsel. How is the data transmitted or disclosed to external organization(s)? Data is produced in a similar fashion as other types of documents are produced to opposing council or law enforcement agencies. Data is exported from Nexidia servers and placed on encrypted media whenever possible such as hard drives, DVD's or CDs.

3. How is the shared data secured by external recipients?
   Enforcement uses encrypted media whenever possible to produce the audio files to external recipients. The recipient is responsible for having adequate controls in place to securely protect the data received.

4. Does the project/system process or access PII in any other SEC system?
   ☐ No.
   ☒ Yes. If yes, list system(s). Nexidia is integrated with CaseMap allowing staff to make entries in their CaseMap databases that point to audio recordings available in Nexidia. It allows investigative staff to link to audio recordings in the CaseMap databases where other evidentiary documents are linked. This allows all important pieces of evidence to be reviewed and tracked in one location.

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice was provided to the different individuals prior to collection of data? (Check all that apply)
   ☒ Privacy Act Statement ☒ System of Records Notice ☒ Privacy Impact Assessment
   ☐ Web Privacy Policy ☐ Notice was not provided to individuals prior to collection

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☐ Yes ☒ No ☐ N/A
   Please explain: Typically individuals or entities are third parties and providing information subject to a subpeona in an enforcement case. Where information is sought from individuals, disclosures are made in such forms as SEC Forms 1661 and 1662. Individuals from whom information is sought voluntarily have the right to decline to provide it. Individuals from whom information is sought via subpoena may decline to provide it based upon an assertion of privilege, Fifth Amendment, or other legal basis. Such assertions may be litigated depending on the facts and circumstances of the assertion.

3. Do individuals have the right to consent to particular uses of the data?
   ☐ Yes ☒ No ☐ N/A

Please explain: Individuals do not have the right to consent to particular uses of the data. As noted above, the routine uses of information are provided to individuals from whom information is sought in SEC Forms 1661 and 1662.

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the National Archives and Records Administration (NARA)?
   ☐ No If no, please explain:
   ☒ Yes If yes, list retention period: Audio recordings are documents, and the retention schedule for Enforcement investigation documents applies. These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with records schedules of the United States Securities and Exchange Commission as approved by the National Archives and Records Administration.

2. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
   Training on the proper use of the system is available through Enforcement. Online help and documentation is also available in the Nexidia software tools. Additionally, all SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII.

3. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date C&A was completed: C&A was performed by OIT in April 2011 to conform to compliance with FISMA requirements. ATO was issued 4/26/11.
   ☐ No If the project does not trigger the C&A requirement, state that along with an explanation

4. Is the system exposed to the Internet without going through VPN?
   ☒ No
   ☐ Yes If yes, Is secure authentication required? ☐No ☐Yes; and
   Is the session encrypted? ☐ No ☐Yes

5. Are there regular (ie. periodic, recurring, etc.) PII data extractions from the system?
   ☐ No
   ☒ Yes If yes, please explain: Analysis reports are presented to the user as a result of the user's search query. These reports may be exported from Nexidia servers to be produced to external parties or for use in ongoing enforcment cases. When exporting data from the system, data is placed whenever possible on encrypted media such as hard drives, DVDs, or CDs.

6. Which user group(s) will have access to the system?
   Enforcement staff. Users are assigned a profile when an account is created (i.e. SEC user, SEC LSS, SuperUser). Super User is granted only to ENF tech support staff for maintenance and operation of the application. The SEC LSS is be granted to all Litigation Support Staff members with general tag administration duties and read only access to Forensic Search. The

SEC USER is granted to all investigative staff working on the related cases. they have read only access to Forensic Search and have the ability to view and assign tags to files.

7. How is access to the data by a user determined? The Enforcement Division determines user access. ENF will send a case request listing staff members that will need access to a particular case to ENF tech support. Access to Nexidia ESI will be granted to limited Enforcement staff who have a need to know by case, in accordance with existing Enforcement procedures.
   Are procedures documented? ☒ Yes ☐ No

8. How are the actual assignments of roles and rules verified.
   All Nexidia users work in the Division of Enforcement and users with access to index data must be assigned to that case. The nature and extent of that access is controlled by the roles within the application and assignment to cases.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? Nexidia uniquely identifies and authenticates users before they gain access to the internal application. Users are required to enter UserID and password for network access to Nexidia. The user account log in will be the same user name the staff member uses to log into active directory and will not require a new password to be created. If the user is not setup in Nexidia, the system requires the user to login before gaining access to the system. As part of the internal technical controls within the system, case files are restricted to those persons with a need-to-know. All accounts are subject to audit logs. In addition, the Division will conduct regular quality assurance and process monitoring activities to ensure adherence to proper security controls and procedures.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

There are a few privacy risks with audio recordings. Nexidia allows audio recordings produced to the SEC from external parties to be loaded in to a database and indexed. There is a risk that this automated process may result in inaccurate data and the collection of more information than needed as related to an individual. The SEC mitigates this risk by validating the data collected against other evidence in the Enforcment case. Nexidia allows the indexed data to be linked in Case-Map and Concordance with other evidentary data to be evaluated for litigation purposes. Enforcement staff can quickly limit the data indexed to only data that is relevent to the pending investigation and link only that data to other data in the case.

Additionally, there is a risk that nonpublic data or PII may be disclosed for an unauthorized purpose or to an unauthorized third party. These risks are mitigated by the common controls in place for the SEC internal network and system-specific controls for Nexidia. The electronic records are protected from unauthorized access through password identification procedures, limited access as per role based and permission level controls, firewalls and other system-based protections, among other appropriate methods. Additionally audit procedures have been implemented which include review of audit logs to ensure appropriate uses.