PRIVACY IMPACT ASSESSMENT

Legal eDiscovery

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: March 2022
(b) Name of system: Legal eDiscovery
(c) System acronym: eDiscovery
(d) Bureau: Office of the Legal Adviser (L)
(e) iMatrix Asset ID Number: 279687
(f) Child systems (if applicable) and iMatrix Asset ID Number:
(g) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

When a case is presented to the court, by either the Department of State or an outside firm, a discovery request for evidence and other pertinent material is made from opposing counsel and the court. This documentation is collected and reviewed by the L-H/EX records team for requesting attorneys and presented in an unstructured format, and is comprised of many data types such as documents, emails, images, video files, etc. The eDiscovery platform provides an electronic platform to aid in this process by ingesting

many different types of electronic documents and content, and providing an efficient document review method.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Name, business contact information, personal phone number, personal email address, personal address, date of birth, place of birth, mother's maiden name, biometric records, social security number.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

5 U.S.C. § 301 (Departmental Regulations)
22 U.S.C. § 2651a (Organization of Department of State)
5 U.S.C. § 552 (Freedom of Information Act)
5 U.S.C. § 552a (The Privacy Act of 1974)
40 U.S.C. § 11315 (Agency Chief Information Officer)
44 U.S.C. § 3506 (Federal agency responsibilities)
42 U.S.C. § 659 - Consent by United States to income withholding, garnishment, and similar proceedings for enforcement of child support and alimony obligations
42 U.S.C. § 666 - Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement
5 CFR part § 581 - Processing garnishment orders for child support and/or alimony
Public Law 71-715

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  STATE-21 - Legal Case Management Records
  STATE-79 - Digital Communication and Outreach

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  STATE-21 20 June 2018
  STATE-79 27 January 2016

☐No, explain how the information is retrieved without a personal identifier.
Click or tap here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  N/A

- Disposition Authority Number:
  DAA-0059-2019-0014-0003
  DAA-0059-2019-0014-0011
  DAA-0059-2019-0014-0013

- Length of time the information is retained in the system:
  Depending on the records and case in question, they may be kept between 1 year and up to a permanent basis.

- Type of information retained in the system:
  Significant case files are those that meet one or more of the following criteria: 1) receives Presidential or Congressional attention; 2) receives considerable public and/or media attention; 3) have an effect on department policy; and/or 4) which establish a principle or rule. This may include records such as correspondence relating to legal briefs, depositions, trial and/or hearing transcripts, exhibits, pleadings, notes, emails, cables, reports, memoranda, article, copes of regulations and legislation, legal opinions, and other court-related records. Topics include, but are not limited to, trade agreements, litigation, extradition, consular affairs, visas, passports, international children's issues, protection and restitution of cultural property, human rights, refugees, United Nations, international traffic in arms, appropriations, foreign assistance, nonproliferation, and Atomic Energy Act.

  Additionally, all case files that do not meet the criteria of significant, including those related to administrative aspects of the department, or routine mission-related activities.

  Finally, records that document the routine non-substantive information relating to legal advice on all legal issues, domestic and international, arising in the course of the Department's work. The records include, but are not limited to, information created and maintained while receiving, coordinating, reviewing, processing, approving and reporting on the day-to-day legal activities that do not contain information of historical value such as department notices, ALDACs, memorandums, action memos, budget and finance statements; pleadings, opinions, briefs and other legal documents brought by or against the Department.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☐ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☒ Other
☐ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?
5 U.S.C. §301 - Departmental regulations
42 U.S.C. 659 - Consent by United States to income withholding, garnishment, and similar proceedings for enforcement of child support and alimony obligations
42 U.S.C. 666 - Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement
5 CFR part 581 - Processing garnishment orders for child support and/or alimony
Public Law 71-715

(d) How is the PII collected?

Any PII in the original records would be contained within the eDiscovery system and would be pulled from existing Department of State records as part of the discovery process. The eDiscovery system does not generate its own records but works with existing Department of State records, which are obtained via a request from the attorney or paralegal who is working on the case file being processed. This begins the data ingestation process. Any information and/or data generated inside Department of State are considered a Department of State record. Any data that are generated outside of Department of State such as text messages, instant messages, pictures of messages, etc. that deal with the case are considered Department of State records and can be included in the discovery process without notifying the owner of the records.

The Office of the Legal Adviser attorneys represent bureaus within the Department (clients) and submit a Nuix Processing Request form through the portal with detailed information on what to do with the documentation that they provide. Once L-H/EX accepts their form, the bureau collects all documentation in correspondence to the case and sends it to their attorney via encrypted email or presents it to their attorney via a shared drive. The attorney then copies the information to a shared drive within L, and the

L-H/EX Records Team ingests the data from the shared drive into Nuix Investigate that is housed within the eDiscovery system server, creating metadata profiles that allows the Office of the Legal Advisor to see the data in the format required, using Optical Character Recognition and deduplicating as needed.

(e) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

(f) What process is used to determine if the PII is accurate?

There is no verification of the accuracy of the PII. The eDiscovery system collects data as are – L does not and cannot make any alterations to the data the eDiscovery system ingests, as that may spoil the data and make them inadmissible.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

There is no verification of the currency of the data. The eDiscovery system collects data as are – L does not and cannot make any alterations to the data the eDiscovery system ingests, as that may spoil the data and make them inadmissible.

(h) Does the system use information from commercial sources? Is the information publicly available?

The system does not use information from commercial sources or information that is publicly available.

(i) How was the minimization of PII in the system considered?

The data collected are limited to a need-to-know basis, however due to the discovery process, the data are ingested as are. The reviewers redact any information that is not pertinent to the case. This generally includes SSNs in order to minimize the amount of sensitive data in the system.

5. Use of information

(a) What is/are the intended use(s) for the PII?

Any PII that is included in the data or evidence requested as part of the discovery process will, and must, be included in the discovery package that is sent to the requesting party, e.g., opposing counsel, etc. for use in discovery proceedings.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes. The PII is required for the discovery process and the eDiscovery system was designed to facilitate the discovery process.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) If the system will use test data, will it include real PII?
☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal: Information is shared with Department staff involved with the case (attorneys, paralegals, and the records management team) who are requesting information as part of the discovery process.

External: Information is shared with opposing counsel, court of jurisdiction, third party contract reviewers, outside counsel and consultants, as required by the litigation and discovery process.

(b) What information will be shared?

Internal: All PII and other information required by the discovery process is shared.

External: All PII legally required by external entities is shared.

(c) What is the purpose for sharing the information?

Internal: Information is shared in order to meet litigation and discovery requirements

External: Information is shared in order to meet litigation and discovery requirements

(d) The information to be shared is transmitted or disclosed by what methods?

Internal: Information is manually copied from the eDiscovery system to a shared network location by the Data Administrators in which permission is granted only to those who have an official need to know.

External: Information is shared via Department approved encrypted storage device or S-FTP site, depending on the external client.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: The permissions on the shared network locations are role and permission based. Access to the eDiscovery system requires a valid Department Active Directory (AD) account, and all Department AD accounts use Multi-Factor Authentication (MFA).

External: Only authorized users who have a need to know are given possession of the encrypted storage media and/or access to the S-applicable FTP site. A valid user account is required to access the S-FTP site.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Notice is not provided to the record subject prior to the collection of information since the system does not collect directly from the records subject but from the existing Department records that were ingested as part of the discovery process.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

The eDiscovery system does not collect the data from the record subject; therefore, they do not have the opportunity to provide consent.

(c) What procedures allow record subjects to gain access to their information?

Individuals are not able to access their information in the eDiscovery system due to its role in the discovery process. They would need to follow the procedures for the source system or source data.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

The record subject would need to address any inaccuracies or errors with their data in the eDiscovery system by following any procedures for the source system or data set. The information must be taken as is for litigation purposes. If the original data were altered, it would be spoiled, making it invalid and potentially inadmissible.

(e) By what means are record subjects notified of the procedures to correct their information?

There are no procedures in place for notification of the data in eDiscovery, as it only ingests data that already exists, and notification may be spoil the litigation and discovery process, making the data inadmissible.

8. Security Controls

(a) How is all of the information in the system secured?

Only authorized users of the eDiscovery system who have an account in the system are able to access the eDiscovery system. All accounts use single sign on via the Departent of State Active Directory directory service. In addition, all access to the eDiscovery system is role-based – only certain roles can perform certain actions such as data ingestion, data review, and system administration.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Data Reviewers – Review and apply certain data processing such as redactions, Bates stamping, etc. Reviewers have access to all of the PII that is contained in the original dataset for the particular case, which may include any of the PII in section 3d.

Data administrators – Gather the data and prepare them for ingestion into the eDiscovery system. The data administrators have access to all of the PII that is contained in the original dataset for the particular case, which may include any of the PII in section 3d. Data Administrators do not review data however, nor is that their role.

System Administrators – Administer the system and ensure it is functional. The systems administrators have access to all of the PII that is contained in the original dataset for the particular case, which may include any of the PII in section 3d. This level of access is present because they have access to the entire eDiscovery system for maintenance and troubleshooting purposes, but they do not review the records contained in the system.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Each case in eDiscovery is insulated from other cases in the system, and the data in each case are protected by an Access Control list that prevents anyone from accessing the case without official need. The data reviewers have access to only the cases that they are currently working on. The data administrators have access to all of the cases, as they are responsible for adding data to the case as requested by the reveiwers. The system administrators have permissions to all of the data in the system for administration and maintenance purposes. The system creates an audit trail that records who performed what actions on a case.

(d) How is access to data in the system determined for each role identified above?

All users of the system must request access through their supervisor. Normally, supervisors do not have access to the eDiscovery system; they are only requesting access for a subordinate. Once the access request has been made, the request must be approved by the Executive Director and the L-H/EX Records Manager for the particular role they will serve in. Additionally, the system administration role request must be approved by the L ISSO.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

Each case in the eDiscovery system is walled off from every other case, and each case is protected by an Access Control List. The system creates an audit trail whereby it can be determined who performed what actions on a case.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All users must also take the annual Cyber Security Awareness course (PS800) and the Records Management for Everyone (PK217), which have privacy components, and the biennial Protecting Personally Identifiable Information (PA318).