AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	Everlaw
1-2	**System Identifier (3 letter identifier):**	EVL
1-3	**Unique Investment Identifier (Exhibit 53):**	FR1916055736
1-4	**Office or entity that owns the system:**	Office of General Counsel (OGC)
1-5	**Office or entity that operates the system:**	Alvarez LLC
1-6	**State if the system is operational or provide the expected launch date:**	Yes
1-7	**System's security categorization:**	Moderate
1-8	**Date of most recent Security Assessment and Authorization (SA&A) or why one is not required:**	Currently undergoing SA&A 2024
1-9	**Approximate number of individuals with Personally Identifiable Information (PII) in the system:**	Everlaw has processed around 15 cases. The files and the information obtained that are used for discovery might contain PII of less than a thousand individuals.

3- SIGNATURES (ORIGINAL MAINTAINED BY CHIEF PRIVACY OFFICER)			
	Role	***Signature***	***Date***
3-1	**Information System Owner:**		
3-2	**Office of General Counsel:**		
3-3	**Chief Privacy Officer:**		
3-4	**Chief Information Security Officer:**		
3-5	**Senior Agency Official for Privacy:**		

4- PIA HISTORY	
4-1	**State whether this is the first PIA for the system or an update to a signed PIA.**
	First PIA
4-2	**If this is an update, describe any major system changes since the last PIA. If this is the first time a PIA is being completed, write Not Applicable.**
	Not Applicable
4-3 A	**State whether this is the annual review of a PIA.**
	Not Applicable
4-3 B	**Describe any changes to the system, data activity, policies, procedures, any interrelating component and process, vendor, third parties, contracts and any required controls since last PIA.**
	Not Applicable
4-3 C	**Describe objects and results of audit or tests (continuous monitoring).**
	Not Applicable
4-3 D	**Certify and state "Completion of Review" if no change occurs.**
	Not Applicable
4-4	**If the system is being retired, state whether a decommission plan is completed and attach a copy.**
	Not Applicable

5- SYSTEM PURPOSE	
5-1	**Describe purpose of the system (or program, product, service)**
	The Everlaw Platform (Everlaw) is a Software as a Service (SaaS) product that combines speed, security, and ease-of-use into a unified, comprehensive solution to unlock the collaborative power of different teams and enables them to investigate issues more thoroughly, uncover truth more quickly, and present their findings more clearly. The Office of General Counsel (OGC) of AmeriCorps uses the Everlaw platform for legal discovery, to search and process electronically stored information (ESI) produced or held by the agency. Everlaw is a single web application that AmeriCorps OGC users access via the internet. The system components are hosted within a Virtual Private Cloud (VPC) in the Amazon Web Service (AWS) GovCloud (US) that is FedRAMP certified.

6- INVENTORY OF PII	
6-1	**Provide a list of all the PII included in the system.**
	The name and email address of AmeriCorps staff who are authorized to access Everlaw are collected and used to set up user account in Everlaw system. The files that AmeriCorps personnel upload to the Everlaw system for discovery might contain PII. These files can be generated from civil ligation, Equal Employment Opportunity administrative complaints, or parallel criminal investigations with which AmeriCorps is a party. In addition, OGC also upload to Everlaw the files extracted by an AmeriCorps discovery tool from AmeriCorps systems to assist OGC staff to search information used for responding to Freedom of Information Act (FOIA) requests. Examples of the categories of data that can be included in these files are biometrics, Social Security number, driver's license number, personal email address and contact information, images of individuals, voice/audio recording, etc.

7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM	
7-1	**Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.**
	The categories of individuals might include AmeriCorps contractors, AmeriCorps federal employees, AmeriCorps volunteer members or program alumni, AmeriCorps prospective employees or volunteer members, or any individuals who are related to a specific case that OGC staffs are assigned to handle. Everlaw has processed around 15 cases so far. The files and the information in Everlaw might contain PII of less than a thousand individuals. However, Everlaw does not maintain the records by using PII as record index.

8- INFORMATION IN THE SYSTEM		
8-1 A	**For each category of individuals discussed above: Describe the information (not just PII) collected about that category and how the information is used.**	
		The Everlaw Platform is a tool used by AmeriCorps OGC staff whose office contact information is required to set up user accounts in Everlaw. The files that AmeriCorps personnel upload to the Everlaw system might contain PII. The files can be generated from investigation of complaints or obtained for discovery of relevant case information and are only used for litigation, administrative adjudication, and FOIA requests. The information relevant to a case or FOIA request will only be shared for permitted purposes in accordance with relevant legal requirements of the jurisdictions where AmeriCorps presents case materials or in records sent in response to a FOIA request.
8-1 B	**State whether the system derives new data, or creates previously unavailable data, about an individual via aggregation of information or other means. Explain why, how it is related to the purpose of the system, how it is used, and with whom it is shared.**	
		Not Applicable
8-1 C	**If the system uses commercial or publicly available data, explain why, how it is related to the purpose of the system, and how it is used.**	
		Not Applicable
8-1 D	**Describe any application of PII redaction, mask, anonymization, or elimination.**	
		For legal or para-judicial investigation and litigation discovery purpose, AmeriCorps maintains relevant case files in Everlaw. All information at rest within Everlaw is encrypted using FIPS-validated cryptography. AmeriCorps would apply PII redaction or/and masking or other appropriate data privacy protection method to protect PII contained in the case files per specific requirements of the jurisdictions that adjudicate the cases or per the Freedom of Information Act.
8-1 E	**Describe any design that is used to enhance privacy protection.**	
		All information within Everlaw is encrypted at rest using FIPS-validated cryptography.

9- COLLECTIONS OF PII INTO THE SYSTEM	
9-1	**Describe for each source of PII in the system:** **a. The source.** **b. What comes from that source.** **c. How the PII enters the system.**

	Authorized AmeriCorps staff's name and email address are required in order to set up their Everlaw Platform user account. The case information can be imported into Everlaw from other systems, applications or devices of AmeriCorps that document certain interactions related to a case between AmeriCorps and the individuals of interest, including the service members or volunteers of AmeriCorps programs or grants, AmeriCorps grantees, AmeriCorps federal staff and contractors, a third party related to a specific case of AmeriCorps', or public individuals. Some case information might be originated from other federal agencies, or administrative adjudicatory organs (for example, parallel criminal investigations with source information from other agencies, such as the United States Attorney's Office) and uploaded into Everlaw. Only AmeriCorps OGC can access the case information in AmeriCorps' Everlaw system.
9-2	**If any PII comes directly from the individual, describe the privacy controls in place. If all PII comes from a secondary source, write <u>Not Applicable</u>.**
	The Everlaw Platform is used to import, store and search case files for discovery and FOIA information search purpose. No PII is directly collected from any individuals into Everlaw. Other AmeriCorps systems, applications, or devices that become a source of information stored in Everlaw might have information that was collected directly from individuals. As required by AmeriCorps' Privacy Policy, all the systems and data handling are subject to strict Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) or Information Sharing Privacy Evaluation processes, and a system of records that is appropriately covered by a System of Records Notice (SORN). These controls ensure that any collection of PII is subject to appropriate privacy controls, i.e., notice and consent, data minimization, and that commensurate data security protection measures are implemented.
9-3	**If PII about an individual comes from a secondary source other than the individual, describe:** **a. Why the PII is collected from the secondary source.** **b. Why the PII from the secondary source is sufficiently accurate.** **c. If/how the individual is aware that the secondary source will provide their PII.** **If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.**
	The files in Everlaw might contain PII; however, Everlaw is not a system of records for any individuals. Some case information might originate from other federal agencies or administrative adjudicatory organs and be uploaded into Everlaw, including, for example, parallel criminal investigations with source information from other agencies, such as the United States Attorney's Office. This source information might contain PII or other information which must maintain its utility by keeping or being able to demonstrate its originality, accuracy, relevancy and completeness. The

	case materials that are used for any legal proceedings or para-judicial processes are subject to further identification, evaluation, verification, and validation processes.
9-4	**If any collections into the system are subject to the Paperwork Reduction Act (PRA), identify the Office of Management and Budget (OMB) Control Number for the collection and effective date. If the system does not implicate the PRA, write Not Applicable.**
	Not Applicable
9-5	**If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write Not Applicable.**
	Not Applicable

10- SYSTEM ACCESS	
10-1	**Separately describe each category of individuals who can access the system along with:** **a. What PII they can access (all or what subset).** **b. Why they need that level of access.** **c. How they would request and receive that access.** **d. How their access is reduced or eliminated when no longer necessary.** **e. Identify policies and procedure outlining roles and responsibilities and auditing processes.**
	The Everlaw Platform is used to search and find relevant documents when OGC processes a case in the discovery phase or identify records to appropriately respond to a FOIA request. Access to the Everlaw system is authorized and granted on job role, based on "need-to-know" and "least privilege" principles. The personnel who is assigned to process the case is authorized to access and use the Everlaw system for that specific case. The Everlaw Platform facilitates targeted information sharing through user-defined groups and fine-grained permissions. Authorized users can use these features to grant specific and restricted authorizations to specific sharing partners for them to access certain information. Depending on the needs of a case, AmeriCorps' personnel can follow procedural requirements to obtain approval for sharing information in the Everlaw system with a party of interest, subject to restrictions set by AmeriCorps. The technical personnel or system administrator of Everlaw might access the system for troubleshooting.

11- PII SHARING	
11-1	**Separately describe each entity that receives PII from the system and:** **a. What PII is shared.** **b. Why PII is shared** *(specify the purpose)* **c. How the PII is shared (what means/medium).** **d. The privacy controls to protect the PII while in transit.**

	e. The privacy controls to protect the PII once received. **f. PII sharing agreements (***describe if the agreement specifies the scope of the information sharing, the parties to the agreement, and the duration of the agreement***)** **g. Describe security and privacy clauses and audit clauses in the agreement or vendor (including third party vendors) contract.** **If PII is not shared outside the system, write Not Applicable.**
	Not Applicable

12- PRIVACY ACT REQUIREMENTS	
12-1	**If the system creates one or more systems of records under the Privacy Act of 1974:** **a. Describe the retrieval that creates each system of records.** **b. State which authorities authorize each system of records.** **c. State which system of records notices (SORNs) apply to each system of records.** **If the system does not create a system of records, write Not Applicable.**
	Everlaw does not create a system of records. Some of the case files that OGC generates might include a component or output obtained from Everlaw through the search and discovery process. AmeriCorps SORN CNCS–01–OGC–Office of General Counsel (OGC) Legal Files covers PII collected in the legal files used and maintained by OGC. AmeriCorps SORN CNCS-02-OGC-FOIA/PA-Freedom of Information Act (FOIA)/Privacy Act (PA) Request Files [84 FR 18268] covers PII collection and processing during FOIA process. Please review these two SORNs for more information.

13- SAFEGUARDS	
13-1	**Describe the data processing environments and the technical, physical, and administrative safeguards (including vendors') that protect the PII in the system.**
	AmeriCorps' Everlaw application is a self-contained "software as a service" (SaaS) application hosted in an AWS VPC and managed by vendor Everlaw Inc. The Everlaw system is safeguarded through multiple layers of control to protect the information in the system. AmeriCorps' information is segregated and stored in its Everlaw instance and is protected by multiple layers of security including layered firewalls, intrusion prevention, and intrusion detection systems. Data is stored on encrypted volumes and can only be accessed after authentication and authorization has passed via Everlaw's privileged management system. All access is logged and alerted for irregularities. IP Switch Outlook Message Encryption (OME) is implemented to delivers encrypted transfer methods to protect data in transit.

		Administratively, all AmeriCorps employees are required to go through annual security and privacy training. The system administrator of Everlaw must sign an AmeriCorps Privileged User Rules of Behavior form and receive privacy and security training annually. The OGC staff can only be approved and authorized to access specific case files that they are assigned to work on. To ensure the system and information in the system are appropriately handled, disposed of, and protected throughout the system and data lifecycle, AmeriCorps identified applicable record retention schedules and responsible personnel to coordinate records retention and disposition. AmeriCorps documents, assesses, and monitors all the privacy and data security measures implemented, to ensure adequate information security and privacy compliance posture are maintained.
13-2	**Describe the technical, physical, and administrative measures that protect PII if the system is being retired.**	
		Not Applicable
13-3	**State if a system security plan and privacy plan is completed and the date of control verification.**	
		The System Security and Privacy Plan (SSP) is completed in June of 2024.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL		
14-1	**Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete, as well as the assurance procedure.**	
		The information used in a discovery process might contain PII. The information must maintain its utility by keeping, or being able to demonstrate, its originality, accuracy, relevancy and completeness. Any information used for any legal proceedings or para-judicial processes are subject to further identification, evaluation, verification and validation processes.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**	
		The case material developed in Everlaw through the discovery process can only be accessed by authorized AmeriCorps personnel. Any information used for any legal proceedings or para-judicial processes are subject to further identification, evaluation, verification and validation processes. Everlaw is not a system of records for any individuals. An individual might view, correct, update, or ask to amend their PII in an AmeriCorps system of records by following the procedures provided in a specific SORN.
14-3	**Describe how an individual could control what PII about themselves is included in the system or how it is used. Also describe how those decisions could affect the individual.**	
		The case material developed in Everlaw through the discovery process is used for litigation or para-judicial processes and for FOIA requests. Such use is included as one of the routine uses in AmeriCorps SORNs and the SORNs for other federal government agencies where the source information might be generated, to which the individuals have consented.

14-4	**State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.**	
		Not Applicable

15- DATA RETENTION AND DESTRUCTION		
15-1	**Identify the National Archives and Records Administration (NARA) provided retention schedule for the system and provide a summary of that schedule.**	
		AmeriCorps records stored within Everlaw are intermediary in nature and are scheduled in accordance with record retention schedule-GRS 5.2, item 020. The disposition authority is DAA-GRS-2022-0009-0002. The records may be destroyed upon creation of the final output record or when no longer needed for business use, whichever is later. Imported source records and output of discovered records are scheduled and retained according to their content by the applicable AmeriCorps records schedule or General Records Schedule (GRS) that are in the process to be identified.
15-1	**Identify the role and process to coordinate with the parties involved in record retention and disposition.**	
		There are 3 sets of records: 1. Input: The original source records – scheduled as applicable to their content. 2. Output: The results (output) documents incorporated into a case file (FOIA or Litigation) – scheduled as applicable to their case file. FOIA-responsive documents are usually scheduled and covered by GRS 4.2/020 and litigation records are scheduled by their applicable AmeriCorps record control schedule. 3. System: The copies of records housed in Everlaw during the systems processing are scheduled as intermediary records covered by GRS 5.2/020. The Information System Owner will coordinate the record retention and disposition activities with the agency records officer.

16- SOCIAL SECURITY NUMBERS (SSNs)		
16-1	**If the system collects truncated or full social security numbers (SSNs):** **a. Explain why the SSNs are required.** **b. Provide the legal authority for the usage of the SSNs.** **c. Describe any plans to reduce the number of SSNs.** **If the system does not collect any part of an SSN, write Not Applicable.**	
		Not Applicable

17- WEBSITES	
17-1	**If the system includes a website which is available to individuals apart from AmeriCorps personnel and contractors, discuss how it meets all AmeriCorps and Federal privacy requirements. If the system does not include a website, write <u>Not Applicable</u>.**
	Not Applicable

18- OTHER PRIVACY RISKS	
18-1	**Discuss any other system privacy risks or write <u>Not Applicable</u>.**
	Not Applicable