PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Everlaw, eDiscovery Platform (Everlaw)

Managing Office: Office of General Counsel (OGC), Office of Management (M).

PIA Approval Date: September 27, 2024

PIA Expiration Date: September 30, 2027

1. Is this a new or revised electronic information system? If revised, describe revisions.

Everlaw Application is a new electronic information system.

The software application platform is a collaborative, cloud-based electronic discovery (eDiscovery), FedRAMP-approved Software as a System (SaaS), and hosted by the Amazon Web Services (AWS) cloud service provider. The Office of General Counsel (OGC), the FOIA/Privacy Office, and the Records Management Office. The platform can be used to respond to requests to collect, preserve, review, redact, and produce documentation as part of various document production requests, including Freedom of Information Act (FOIA) requests, document review and production (DR&P), Congressional Oversight requests, litigation, administrative records preparation, and possibly investigations. Everlaw serves as an online document repository that is used to filter through all documents that may be responsive to a request. The system will also assist in records management requirements.

The eDiscovery tool will also assist the agency in become more compliant with federal Records Management requirements that include but not limited to:

- 44 USC 3102 c.1 “Agency records management program must provide for effective controls over the creation, maintenance, and use of records in the conduct of current business”

- OMB-19-21 which requires that all federal agencies manage records created or received electronically in an electronic format.

- Managing electronic records in accordance with Government-wide requirements including managing all email records electronically and retaining them in an appropriate electronic system that support records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as needed (OMB A-130.5.h.3).

• Ensure that federal information is properly managed throughout its life cycle, including all stages through which the information passes, such as: creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition (OMB A-130, 5e.1.a)

2. Identify who the Personally Identifiable Information (PII) is collected from:

_X_ Members of the public, including Peace Corps Volunteer applicants and interns

_X_ Federal employees/federal contractors/Peace Corps Volunteers

_X_ Both members of the public and Peace Corps personnel

3. Legal Authority. Cite the legal authorities that permit and authorize the collection of this information by this IT system.

- OMB Circular A-130, *Managing Information as a Strategic Resource* (July 27, 2016)
- Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service* (April 27, 2011)
- Executive Order on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* (December 21, 2021)
- OMB M–23-22 *Delivering a Digital-First Public Experience* (September 22, 2023)
- OMB M-13-13, *Open Data Policy-Managing Information as an Asset* (May 9, 2013)
- Presidential Directive, *Building a 21st Century Digital Government* (May 23, 2012)
- The Clinger-Cohen Act of 1996, 40 U.S.C. 1401
- 36 CFR 1220: Federal Records, General

4. Purpose. Explain the purpose of the system (e.g., nature and source).

The application is a SaaS FedRAMP-approved SaaS product from Everlaw, Inc. The Everlaw platform consists of a single web application accessed via the Internet. The system components are hosted within a virtual private cloud (VPC) network in the AWS GovCloud (US). Everlaw relies on AWS to provide appropriate physical and logical protections and processes for the AWS GovCloud (US) data center facilities.

It is a collaborative, cloud-based e-discovery and investigation platform that enables government attorneys, and FOIA and records management teams to discover, code, redact, tag, index, and deduplicate data, and act on information to drive internal investigations better, respond to FOIA requests faster, and positively impact the outcome of litigation. Everlaw can receive the documents in numerous formats, including Microsoft Office documents, emails, PDFs, and other formats that are provided by staff

or directly extracted from M365 or other platforms. Everlaw stores the search results in their native formats and allows for easier processing and data productions.

The Everlaw application handles typically complicated and technically demanding processes through wizard-driven workflows. These walk users through the steps to process data, generate assignments and predictive coding models, and finally run productions. The Everlaw application includes a post-review case organization tool, Story Builder. With Story Builder, attorneys can craft narrative timelines of key documents, draft deposition outlines with drag-and-drop document links, collaborate in real-time during depositions, and highlight transcript testimony, all in a central location.

5. List all forms of Personally Identifiable Information (PII) that is collected, maintained, or disseminated. *Examples include first name, middle name or initial, last name, alternate names, birth date, place of birth, Social Security Number (full or partial), personal telephone number, personal address, personal email address, residency during service or host family address, family member information or third person contacts, driver's license number, passport number, Peace Corps Volunteer number, other ID number, gender/gender preference, race or ethnicity, religious preference, marital status, military service status or military records, legal, security, or law enforcement information or status, disability information or status, financial information, educational information, IEP address, MAC address, biometrics, photograph, electronic Protected Health Information.*

The Everlaw application will collect, generate and retain PII that includes but is not limited to: volunteers and RPCVs names, addresses, telephone numbers, banking information, medical information, place of service, current and former employees names, addresses, telephone numbers, banking information, medical information, pay and other personnel information, contractors' and attorneys' names, addresses, telephone numbers, citizenship, gender, birth date, marital status, race or ethnicity, Peace Corps Volunteer number, biometrics, social security numbers, employee and contractor employment information,, military service records, disability information, education information, gender preference, child or dependent care, photographs, chat and voicemail information, and other PII from individuals who do business with the agency. Due to the nature of Everlaw document processing for different programs and missions, there may be numerous PII on the original documents that are reviewed.

6. Why is PII being collected (e.g., to determine eligibility)? Does the IT system collects PII directly from individuals, or from another system?

The system collects PII to help with investigations, FOIA requests and for litigation purposes. The system does not collect information directly from individuals. The system collects information directly from the agency's database systems.

7. Sharing and Disclosure.

a. Will the PII from this system be shared with another agency? If yes, list the agency, all types of PII that is shared, and why this is shared outside our agency.

Other federal agencies do not access the PII directly, except for the U.S. Department of Justice for litigation purposes. The records maintained in the Everlaw system are copies of documents pulled from other sources, which are used for document production purposes, such as for investigations, Congressional inquiries, litigation support, FOIA, and records management. Authorized users will review document collections to determine what needs to be redacted and what is appropriate for release, depending on the litigation, specific requests and records management requirements. Information may be shared with other Federal agencies as authorized and required to meet legal and reporting requirements in accordance with the Privacy Act of 1974, as amended, system of records notices (SORNs) or any other applicable requirements.

b. Is the sharing pursuant to a Memorandum of Understanding, Computer Matching Agreement (CMA), or other type of approved sharing agreement with another agency?

No.

8. Notice of the collection of information.

a. Do individuals have the opportunity to object or to consent to the particular use of their PII prior to collection?

__ Yes _X_ No

b. If "Yes," describe the Privacy Act Statement (PAS) or notice provided to the individual prior to collection of his or her information. If "No," state the reason why individuals cannot give or withhold their consent. Identify if this is not applicable because information is obtained from an existing information system or source.

Everlaw is a records query and collection system and does not collect PII directly from the individual. Rather, the information is collected from various Peace Corps systems and records, which do not provide individuals with an opportunity to decline to provide information in the records collection and management process.

c. List any Peace Corps form(s) or federal form(s) used to collect PII for this system. Each PC form must have a Privacy Act Statement.

N/A

d. Provide the OMB Control number and the agency number for the collection if this collection is covered by the Paperwork Reduction Act (PRA).

N/A

9. Security.

a. What administrative, technical, and physical security safeguards/controls are in place to protect the PII?

The privacy risks associated with this IT system are unauthorized access and unauthorized disclosure of PII. Administrative, physical security and technical safeguards are in place to mitigate these risks. This FedRAMP-authorized system has undergone review and authorization of administrative, technical, and physical security safeguards and controls. Security control assessment is also conducted on an annual basis by the vendor to ensure the security controls are still working as intended and are yielding desired outcomes**.**

Administrative Controls: Access to the application is prohibited without identification and authorization. Only authorized personnel will have restricted access to the application and its information, based on a need-to-know basis, to fulfill official duties. Everlaw (vendor) creates administrator accounts for the Everlaw Platform on the front-end web portal. The PC will assign administrator that manages any additional Everlaw Platform account creation and management processes at the application level. Access to the application will only happen after access has been granted to the application by the application administrators. The administrator assigns user roles to personnel with an official need to know to perform their duties within the system. Authorized users are trained in properly handling personally identifiable information and their official responsibilities under the Privacy Act and Peace Corps technical governance for the rules of behavior. The vendor, Everlaw, has access to the data in the capacity of the administrator and service provider for the system.

Physical Controls: The appropriate controls are in place to ensure that the vendor’s server location adheres to all physical security requirements. This includes measures to protect the physical integrity of server infrastructure against unauthorized access or environmental threats.

Technical Controls: Access to this application will be through the use of single sign-on (SSO) that will be integrated with PC Active Directory Federated Services (ADFS), which allows for users' identity to be verified based on their credentials within PC ADFS, and this supports the use of MFA for access. Everlaw SSO uses the Security Assertion Markup Language (SAML) 2.0 protocol, which ensures the process of exchanging authentication and authorization data between ADFS, and application is secured as it uses HTTPS, which ensures the entire communication is encrypted. The application supports the granular level of permission that tailors access rights to users' specific needs and ensures that users have exactly the level of access necessary for their role. Everlaw customers’ data is encrypted, whether it is in transit or at rest. In Transit,

Everlaw serves application data using HTTPS to ensure encryption of all customer data. The Everlaw application uses Transport Layer Security (TLS) version 1.2 or higher to protect HTTPS communications. At rest, Everlaw leverages the default encryption at rest provided by AWS, which protects the data on disk with AES-256 encryption. They also configure all snapshots to encrypt backup data.

Each host is configured according to a deny-all, permit-by-exception methodology. The security groups control the IP addresses that can interact with the machine and the authorized ports, protocols, and services allowed to be accessed on each component. The Federal Information Processing Standard (FIPS) 199 security impact category for this system is moderate. By combining these physical, administrative and technical controls, the PC ensures that access to the application is both secure and efficient, providing users with the necessary tools while safeguarding sensitive information.

b. Has a system security plan been completed for the information system?

No, this is a new system, and the OCIO team is preparing the system for a security assessment and to complete the SSP and obtain an Authorization to Operate (ATO).

10. Privacy Act System of Records. Identify the System of Record Notice (SORN) that covers this IT system, or state if a SORN will be created under the Privacy Act, 5 U.S.C. 552a.

The agency has not yet created a SORN for the Everlaw system.

11. Records Retention and Disposition. Identify the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system, or for the records maintained in the system, as well as the record retention instructions.

Legal Advice and Guidance Records (Disposition Authority: DAA-0490-2017-0011-0004)
Routine legal advice, activities, and guidance regarding issues affecting Peace Corps offices and posts. Records include summaries of issues, recommendations, comments, drafts, overseas legal counsel interviews or other notes, and correspondence.
DISPOSITION: Temporary. Cut off at the end of the calendar year. Destroy 7 years after cutoff

Access and Disclosure Request Files DAA-GRS-2016-0002-0001, GRS 4.2 Item 020:

Case files create in response to requests for information under the Freedom of Information Act, and Privacy Act.

DISPOSITION: Temporary – Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.