U.S. Immigration and Customs Enforcement

REQUEST FOR INFORMATION (RFI) #ICE-03162020

eDiscovery Software as a Service (SaaS)

1.0 Background

The Office of the Principal Legal Advisor (OPLA), a component within the Immigration and Customs Enforcement (ICE) federal agency, is the largest legal program in the Department of Homeland Security (DHS), with over 1,100 attorneys and 350 support personnel. By statute, OPLA serves as the exclusive representative of DHS in immigration removal proceedings before the Executive Office for Immigration Review, litigating all removal cases including those against criminal aliens, terrorists, and human rights abusers.

OPLA also provides a full range of legal services to ICE programs and offices. OPLA provides legal advice and prudential counsel to ICE personnel on their customs, criminal, and immigration law enforcement authorities, the Freedom of Information Act and Privacy Act, ethics, legal liability under the Federal Tort Claims Act, and a range of administrative law issues, such as contract, fiscal, and employment law. OPLA represents the agency before the Merit Systems Protection Board, the Equal Employment Opportunity Commission, and the Board of Contract Appeals. OPLA attorneys provide essential support to the Department of Justice in the prosecution of ICE cases and in the defense of ICE's authorities in federal court.

In addition to its headquarters in Washington, D.C., OPLA has 25 Offices of Chief Counsel with a presence in more than 60 locations throughout the United States.

ICE OPLA handles a large volume of cases and associated data. ICE handles all aspects of the electronic discovery lifecycle using Relativity software which is presently deployed and hosted in the Microsoft Azure cloud environment. Relativity is used for the processing, analysis, review, and production of potentially relevant data as part of the discovery phase in litigation, compliance with FOIA requests, or in the course of investigations and Congressional requests and inquiries.

ICE is seeking to transition to an eDiscovery platform based on a Software as a Service (SaaS) model. The host environment must be ***FedRamp certified or in the process of obtaining FedRamp certification with a federal sponsoring agency***.

2.0 Purpose of Request for Information

THIS IS A REQUEST FOR INFORMATION (RFI) to identify sources that can provide eDiscovery Software in a (SaaS) model on a subscription basis in an environment certified to host Federal data and records. This RFI is issued solely for information and planning purposes – it does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This request for information does not commit the Government to contract for any supply or service whatsoever. Further, ICE will not accept unsolicited proposals. Interested parties are advised that the Government will not pay for any information or administrative costs incurred in response to this RFI. All costs associated with responding to this RFI are incurred solely at the interested party's expense and remain that party's responsibility. If an RFP is released, it will be posted on e-GOS/Beta.Sam. It is the responsibility of the interested parties to monitor these sites for additional information pertaining to this requirement. All submissions become Government property and will not be returned. Responses to the RFI may be used to develop Government documentation. DO NOT submit pricing information in response to this RFI.

3.0 Description of Requirements

ICE is exploring procurement strategies for the use of electronic discovery software in a SaaS based offering hosted in a FedRamp certified environment. ICE seeks information from all parties that currently offer this service and are FedRamp certified or are in the process of obtaining

Based on current eDiscovery practices and procedures, ICE anticipates acquiring capabilities that meet the following high-level tasks:

Task 1: Identification and Preservation of Data

Task 2: Collection of Data

Task 3: Processing

Task 4: Analytical Features and Functionality

Task 5: Review and Redaction of Data

Task 6: Production of Data

4.0 Process

This RFI is being conducted as a two-step process. The first step is for interested parties to provide the information requested in Section 5.0 White Paper Submission.

After reviewing White Paper Submissions, ICE may contact interested parties to participate in One-on-One sessions. One-on-One Sessions will be conducted as outlined in Section 6.0 Industry One-On-One Sessions.

5.0 White Paper Submission

Interested parties are requested to respond to this RFI with a white paper. Responses must be submitted in size 12 Times New Roman font with single spacing and 1" margins. The white paper shall include the following:

5.1 Administrative Information (no page limit)

At a minimum, interested parties shall provide shall include the following:

- Name, mailing address, DUNS number, phone number and e-mail of designated point of contact.
- Current Information Technology contract vehicles that your company holds such as EAGLE II, Alliant, Alliant SB, GSA Schedule, etc.
- Business type based upon North American Industry Classification System (NAICS) code 541512, Computer Systems Design Services (large business, small business, small disadvantaged business, etc.)
- Identify if your company is interested in participating in a One-on-One session with the Government.

5.2 Question Responses (20-page limit)

Interested parties shall address all the questions outlined below.

General Software Features/ SaaS Environment:

1. How are backups performed and how frequently?
2. What are the client's administrative responsibilities? What system admin functions are provided as part of the subscription?
3. Are there features/functionality that are provided which are charged in addition to the subscription fee?
4. What are the policies and availability of third-party add-ons (e.g. use of mass redaction features provided by Milyli Blackout product)?
5. Where is the data hosted (Azure, Amazon Web Services, etc…)?
6. What technical support services are provided as part of the subscription? (please explain in detail).

7. Do you provide tools and/or services to assist clients in migrating existing data to your environment?
8. Do you offer litigation hold functionality in a SaaS model? If so, how would this be integrated with MS Office 365 service? How will existing Preservation Notices be migrated?
9. Do you provide guaranteed server uptime in terms of percentage of time system will be guaranteed to be up and running?
10. Are user licenses concurrent or named?
11. Do you offer different storage/hosting rates (active/archived/offline)?
12. Do you provide offline loading of data?
13. Provide a general description of the subscription pricing/model.
14. What are the various login procedures/protocols offered? (RSA tokens, two-factor authentication, etc…)
15. Are there fees associated with the uploading and downloading of data to your environment, data transit fees?
16. What is the schedule and policy on version upgrades and application of patches?
17. Does the subscription fee include processing/imaging/indexing/production of data?

Security Related Questions:

1. Type of FedRamp ATO (JAB or Agency)
2. Please confirm GSS classification (availability = high, Confidentiality = high and integrity = high)
3. Do you have a group of security officers to perform scan analysis?
    a. What is the frequency for scanning (web, application, database and operating system)?
    b. Who will be responsible for remediation of discovered vulnerabilities?
    c. How will vulnerabilities be managed and tracked?
    d. How often are scans performed?
4. What is the encryption used for data in transit?
5. What is the encryption used for data at rest?
6. How is access control implemented?
    a. Who is responsible for access control?
    b. Who will be creating, modifying, disabling accounts?
    c. Are automated mechanisms used for account management?
        - Disabling inactive accounts
        - Creating new accounts
        - Modification to an account
7. Who will perform audit log review?
    a. What tool will be used for audit log review?
    b. What actions will be taken for audit processing failure?
    c. What actions will be taken for audit log anomalies?
8. Who will provide the configuration management plan?
    a. Provide the hardening guide used to secure the system?
    b. How will inventory control be handled?
9. How will users be authorized to use the system?
    a. How will users be identified?

    b. Will PIV be used?
10. What is used to protect the database from unauthorized access or modification?
11. How will the vendor implement DHS Policy as stated in the DHS 4300A?
12. Who will prepare the contingency plan?
    a. How is contingency training conducted?
    b. What method will be used for contingency plan testing?
13. Will there be a POC for system management?
    a. What is the frequency for patching?
    b. Who will be performing updates to on-prem or ICE administered applications used by the eDiscovery software?
    c. Who will be performing updates for the OS?
    d. Who will be performing updates for the database?
    e. Who will be archiving data?
        - How will archived data be protected?
    f. Who will be performing backups?
    g. How will rogue devices be detected and what isolation techniques will be used?
14. Will there be a POC for system security?
15. How will incident response be conducted?
    a. Who will be notified?
16. What methods will be used to protect OPLA's data from other hosted companies/agencies?
17. What intruder detection methods will be used?
18. What protection from malicious software?
19. How will the OPLA data be controlled?
20. What will be the network disconnect time period for inactive users?
21. Will session lock be utilized for inactive users?
22. What will used to prevent denial of service and other malicious attacks?

6.0 Industry One-On-One Sessions

The Government, at its own discretion, may use the white paper responses received as the basis to identify candidates for the One-on-One sessions. The Government will not conduct One-on-One sessions with companies that do not submit a white paper in response to this RFI. Due to limited resources, every interested party that submits a white paper will not be guaranteed a One-on-One meeting. Therefore, interested parties are asked to provide substantive responses to the questions on the white paper.

One-on One sessions will be conducted according to the ground rules identified below:

1. Both the Government and interested party will communicate with honesty, integrity, and confidentiality.
2. Government resources to perform this effort are limited, therefore there will be only one session per company.
3. No marketing efforts. The intent of this effort is to discuss issues and generate ideas affecting ICE's agile development procurements, not to discuss company capabilities.
4. Participation in this process is strictly voluntary.
5. Participation in this effort will have no bearing on future awards of contracts for eDiscovery on a SaaS basis.
6. One-on-One sessions will generally last 1-2 hour(s). The content of the One-on-One sessions will be centered around the features/functionality and environment of the

eDiscovery SaaS offering.

7. One-on-One sessions may be conducted in person in the Washington DC metro area, or via teleconference as Government resources allow.
8. The Government will notify each RFI responder whether they have been selected for a One-on-One session and if selected, the date, time, and location of the session.

7.0 Questions

Questions and requests for additional information must be sent to DHS/ICE via e-mail to: Contract Specialist, Deanna.Brassard@ice.dhs.gov and Contracting Officer Jina.Jackson@ice.dhs.gov by Tuesday, March 24, 2020 at 10:00 AM. All submissions shall include in the subject line "RFI #ICE-03162020-eDiscovery (SaaS) – (Company's Name)." Verbal questions will NOT be accepted. Questions shall NOT contain proprietary or classified information. The Government does not guarantee that questions received after the due date deadline will be answered.

8.0 Submission Instructions

Responses shall be received via e-mail as one electronic submission in Adobe PDF format with the subject line "RFI #ICE-03162020-eDiscovery (SaaS)."

Submissions must be received no later than Monday, April 6, 2020 at 10:00 AM and submitted only to: Contract Specialist, Deanna.Brassard@ice.dhs.gov and Contracting Officer Jina.Jackson@ice.dhs.gov. Early submissions are encouraged. ICE reserves the right to review late submissions but makes no guarantee to the order of, or possibility for, this review.

All company proprietary information, performance capabilities and/or future modifications must be clearly identified and marked so segregation of proprietary information is required.