

(A) PURPOSE

This Request for Information (RFI) is for market research, information, and planning purposes **ONLY**. This RFI does not in any way constitute a Request for Proposal (RFP) and as such, shall not be construed as a commitment by the Government (implied or otherwise) to issue a solicitation or ultimately award a contract.

This announcement is specifically targeted for qualified contractors that can perform the services detailed in the **DRAFT** Statement of Work (SOW) dated July 31, 2017. However, responses from all interested parties are appreciated and accepted.

(B) DESCRIPTION OF THE REQUIREMENT

U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) Targeting Operations Division (TOD) has a requirement to obtain mission-critical commercial subscription data services to conduct customized analysis, screening, and monitoring of Department of Homeland Security (DHS) priority criminal alien information. The TOD will provide targeting information for the provider to set up in a continuous monitoring and alert system to track 500,000 identities per month for specified new data, arrests, and activities.

The continuous monitoring and alert system must be able to securely process and return information and addresses using the following types of specified data: FBI numbers; State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; Vehicle Registration Information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN) data; and employer records.

The Government anticipates awarding a Firm Fixed Price type contract for a twelve (12) month period of performance with a six (6) month option period (per FAR clause 52.217-8, Option to Extend Services).

(C) REQUESTED INFORMATION

- 1) Please provide your company's name, mailing address, Cage Code, and Data Universal Numbering System (DUNS) identification number.
- 2) Please provide a brief technical capabilities statement to summarize your company's experience and ability to provide customized analysis, screening, and monitoring services.
- 3) Please provide the primary North American Industry Classification System (NAICS) code that your company utilizes for customized analysis, screening, and monitoring services.
- 4) Please summarize any barriers/challenges you believe your company would encounter in providing customized analysis, screening, and monitoring services for ICE.
- 5) Is your company a small or large business? If small, is your firm classified under a specific socio-economic status?
- 6) Please identify any GSA Schedule contract or other current government-wide contract (e.g., GWAC or BPA) that your company currently holds.
- 7) Has your company had experience with the customized analysis, screening, and monitoring services detailed in the attached **DRAFT** SOW in the last five (5) years?

- 8) Does your firm have any other general feedback and/or applicable information that it would like to provide? If so, please provide the information.

(D) ADDITIONAL GUIDANCE

The Government will not reimburse respondents for any costs associated with information submitted in response to the RFI. Responders are solely responsible for all expenses associated with responding to this RFI.

Responses to this RFI are not offers and cannot be accepted by the Government for the basis of forming a binding contract. This RFI is being issued solely for the purpose of gathering information for planning purposes. This RFI does not commit the Government to a contract for any supply or service. Furthermore, the Government is not at this time seeking proposals and will not accept unsolicited proposals.

Interested parties (specifically small businesses) are encouraged to respond to this RFI. If the scope of this RFI is too large or there are aspects to which your company does not wish to provide a response, please feel free to provide partial/limited feedback in the areas of your specific expertise. ICE hopes to receive information from all interested parties on any aspect of this RFI that could be of benefit to the Government.

Respondents to this RFI may be requested to provide additional information/details based on their initial submittals. The Government reserves the right to select, one (1), some, or none of the submissions for further information. Contractors who submit information in response to this RFI do so with the understanding that U.S. Government personnel may review their materials and or data.

(E) QUESTIONS

Questions regarding this RFI shall be submitted in writing by e-mail to the Contract Specialist and Contracting Officer at Cornell.House@ice.dhs.gov and Benjamin.Shih@ice.dhs.gov. Questions over the telephone will **NOT** be addressed and shall **NOT** contain proprietary or classified information. Questions submitted after 3:30pm (EST) on August 11, 2017 will **NOT** be addressed.

(F) HOW TO RESPOND

Your firm's response **MUST** be provided no later than 3:30pm (EST) on August 25, 2017 and should be emailed to Cornell.House@ice.dhs.gov and Benjamin.Shih@ice.dhs.gov.

TARGETING OPERATIONS SUBSCRIPTION DATA SERVICE REQUEST

REQUIREMENT:

The purpose of this Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) Targeting Operations Division (TOD) request is to obtain mission-critical commercial subscription data services to conduct customized analysis, screening, and monitoring of Department of Homeland Security (DHS) priority criminal alien information. The TOD will provide targeting information for the provider to set up in a continuous monitoring and alert system to track 500,000 identities per month for specified new data, arrests, and activities.

The continuous monitoring and alert system must be able to securely process and return information and addresses using the following types of specified data: FBI numbers; State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; Vehicle Registration Information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN) data; and employer records.

The vendor must have a multi-tiered internal vetting system in place. Specifically, ERO's data must be analyzed internally by both automation and trained analysts with research support tools to provide the best leads possible and to reduce the number of false positives forwarded to the TOD.

Availability of the contracted services must be flexibly structured to adapt to changing priorities in the law enforcement continuum. This flexibility must allow for possible increases or decreases in the amount of the various services needed.

BACKGROUND:

The arrest, detention, and removal of criminal aliens that meet current ICE priorities from the United States are a national priority. To address this priority, ICE formed the Targeting Operations Division within the ICE Enforcement and Removal Operations (ERO) directorate. One of the primary missions of the Targeting Operations Division is to identify and locate aliens that pose a threat to public safety and/or national security.

In 2006, ERO first obtained subscription access to commercial database aggregators provided through an agreement with the Federal Library and Information Network (FEDLINK) managed by the United States Library of Congress. At that same time, ERO also purchased a customized batch service with the capability to vet alien information through commercial databases in a batch process, and obtained access to a custom alert service designed to continuously monitor criminal alien information for recent credit or other commercial activities.

Similar contracts were acquired and managed by ERO in 2007, 2008, and 2009. In 2010, all subscription services obtained for ICE programs were managed by the DHS Library Program Management Division as part of a DHS efficiency initiative.

The growing need for more criminal information and for more accuracy in the batch process prompted the TOD to seek alternatives to data service products currently available through the DHS Library.

JUSTIFICATION:

The proposed support subscription services contract is required to support national ICE initiatives, maintain the efficiency of the Targeting Operations Division, and develop leads which permit ERO Field Offices and other ICE entities to focus resources on priority cases involving aliens that pose a threat to public safety and/or national security.

Successful law enforcement operations require adaptation to changing public safety threats and the ability to continually refine processes and modernize information technologies. Although ICE continues to make considerable progress in identifying and arresting criminal aliens, the continued use of proactive and modern enforcement tools and batch and alert capabilities remains an essential approach to achieve ICE enforcement goals. Other less comprehensive and less efficient approaches to the challenges associated with identifying and locating criminal aliens have resulted in limited success.

Accordingly, the ICE-ERO Targeting Operations Division is seeking a contract service provider to provide a continuous monitoring and alert service that provides real-time jail booking data to support the identification and location of aliens who pose a threat to public safety and/or national security.

CONTRACT LINE ITEMS:

CLN 01 Continuous Monitoring and Alert System (500,000 identities)

Vetting Support Team

PUBLICLY-AVAILABLE AND COMMERCIAL SOURCE SEARCHES AND SEARCH RESULTS

The contractor shall track daily address changes and credit activities of targeted persons (i.e. new aliases, new addresses, new jail bookings, insurance claims, DOB changes, SSNs, etc.) using information available from open sources and commercial data sources. Source listings for this information shall include, but is not limited to, the following: insurance/auto insurance; property; phones; employment; utilities; moving companies; renter information;; drivers licenses; credit checks; vehicle accident reports; Real Time Jail Bookings; pay day loans; check cashing; and death registries.

The contractor shall securely return to ICE from publicly available and commercial sources available to the contractor, any information that identifies the possible location of the target and

changes in the target's identifiers, such as addresses, phone numbers, email addresses, user names, new aliases, date of birth changes, SSN changes, utility changes, arrests, credit checks, death registry information, employment changes, insurance changes, and affiliated organizations through which a location can be derived.

Whether conducting publicly available or commercial source-based searches, the contractor shall not maintain any data, including the list of targets provided by ICE and search results provided to ICE after the analysis is complete, nor shall the contractor maintain any data on behalf of ICE after the data is no longer in a state of analysis. The contractor is also not permitted to use any law enforcement information provided by ICE for any outside commercial purpose.

RELEASE OF INFORMATION

Contractor access to proprietary and Privacy Act-protected information is required under the SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the Privacy Act of 1974, and the *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*. Contractor and subcontractors shall not hold any discussions or release any information relating to this contract to anyone not having a direct interest in performance of this contract, without written consent of the Contract Officer (CO) and Contract Officer's Representation (COR). This restriction applies to all news releases of information to the public, industry or Government agencies, except as follows: Information for actual or potential subcontractors or other individuals necessary for Contractor's performance of this contract. Contractor and subcontractors shall not issue advertisements about projects performed under this task without government review and approval. For the purposes of this paragraph, advertisement is considered to be Contractor-funded promotional brochures, posters, tradeshow handouts, world-wide-web pages, magazines, or any other similar type promotions.

NON-DISCLOSURE

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of these tasks and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of these tasks. Contractors shall be required to sign Non-Disclosure statements.

All information, including documents, workflows, products, training materials, or programs, created in support of ERO, at the request of the TOD management or staff, or generated as a result of this contract, will become the property of the ICE and the U.S. Government.

Data Use, Disclosure of Information and Handling of Sensitive Information

The contractor will not be provided with any classified information through this requirement. However, the contractor will be provided with law enforcement sensitive information. The Contractor shall maintain, transmit, retain in strictest confidence, and prevent the unauthorized duplication, use, and/or disclosure of information. The Contractor shall only provide information to employees, Contractors, and subcontractors having a bona fide "need to know" in the performance of their duties related to this project.

Information made available to the contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other manner without the written agreement and consent of the Contracting Officer.

If public information is provided to the contractor for use in performance or administration of this effort, the contractor, except with the written permission of the Contracting Officer, may not use such information for any other purpose. If the contractor is uncertain about the availability or proposed use of information provided for the performance or administration of the contract, the contractor will consult with the COTR regarding use of that information for other purposes.

The contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each offeror or employee of the contractor to whom information may be made available or disclosed shall be notified in writing by the contractor that such information may be disclosed only for the purposes and to the extent authorized herein.

Performance of this effort may require the Contractor to access and utilize data and information proprietary to a Government agency or Government Contractor, which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others.

Contractor and/or Contract personnel shall not divulge or release data or information developed or obtained in performance of this effort, until such time as it is made public by the Government. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort.

PERIOD OF PERFORMANCE:

The period of performance shall be 12 months.

The Government reserves the right to modify performance standards and/or metrics during the life of this contract, in order to ensure that the right outcomes are being assessed and that the performance standards are appropriate. Any changes will be accomplished by bilateral contract modification.

The Government may terminate performance of work under this contract in whole or, from time to time, in part if the Contracting Officer determines that a termination is in the Government's interest. The Contracting Officer shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date.

Unauthorized Commitments (FAR 1.602.3)

The Contracting Officer's Representative (COR) is designated by the Contracting Officer (CO) to perform as a technical liaison between the Contractor's management and the CO in routine technical matters constituting general program direction within the scope of the contract. Under no circumstances is the COR authorized to effect any changes in the work required under this contract whatsoever or enter into any agreement that has the effect of changing the terms and conditions of this contract or that causes the Contractor to incur any cost.

Notwithstanding this provision, to the extent the Contractor accepts any direction that constitutes a change of this contract without prior written authorization of the Contracting Officer; costs incurred in connection therewith are incurred at the sole risk of the Contractor and if invoiced under this contract

will be disallowed. On all matters that pertain to the contract terms, the Contractor must communicate with the CO.

Whenever, in the opinion of the Contractor, the COR requests efforts beyond the terms of the contract, the Contractor shall so advise the CO. If the COR persists and there still exists a disagreement as to proper contractual coverage, the CO shall be notified immediately, preferably in writing. Proceeding with work without proper contractual coverage may result in nonpayment or necessitate submittal of a contract claim.

PRIVACY AND RECORDS REQUIREMENTS

PRIV 1.2: Reporting Suspected Loss of Sensitive PII: Contractors must report the suspected loss or compromise of Sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of Sensitive PII.
2. The Contractor must report the suspected loss or compromise of Sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.
3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of Sensitive PII by its employees or Subcontractors. The report must contain the following information:
 - a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
 - b. Date, time, and location of the incident.
 - c. Type of information lost or compromised.
 - d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
 - e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
 - f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
 - g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
 - h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.
4. The Contractor must cooperate with ICE or other Government Agency inquiries into the suspected loss or compromise of Sensitive PII.
5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access Sensitive PII or to work on that contract based on their actions related to the loss or compromise of Sensitive PII.
(End of clause)

PRIV 1.3: Victim Remediation: The Contractor is responsible for the notification of victims and the provision of victim remediation services in the event of a loss or compromise of Sensitive PII held by the Contractor, its agents, and its Subcontractors, under this contract. The victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as requested by the Government, call center help desk services for the individuals whose Sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.
(End of clause)

PRIV 1.7: Privacy Act Information: In accordance with FAR 52.224-1, PRIVACY ACT NOTIFICATION (APR 1984), and FAR 52.224-2, PRIVACY ACT (APR 1984), this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974. The Agency advises that the relevant system of records notices (SORNs) applicable to this Privacy Act information include, but are not limited to:

DHS / ICE 011 –ENFORCE SORN

These SORNs may be updated at any time and the most current versions are publicly available at www.dhs.gov/privacy.
(End of clause)

REC: 1.1: Required DHS Basic Records Management Training: The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to Sensitive PII as well as the creation, use, dissemination and/or destruction of Sensitive PII at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site. The Agency may also make the training available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance. The Contractor must submit an annual e-mail notification to the Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.
(End of clause)

REC 1.2: Deliverables are the Property of the U.S. Government: The Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable without the expressed permission of the Contracting Officer or Contracting Officer's Representative. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract. The Agency owns the rights to all data/records produced as part of this contract.
(End of clause)

REC 1.3: Contractor Shall Not Create or Maintain Unauthorized Records: The Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records. The Contractor shall not create or maintain any records containing any Government Agency data that are not specifically tied to or authorized by the contract.
(End of clause)

REC 1.4: Agency Owns Rights to Electronic Information: The Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation created as part of this contract. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the Agency to use the data.
(End of clause)

REC 1.5: Comply With All Records Management Policies: The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.
(End of clause)

REC 1.6: No Disposition of Documents without Prior Written Consent: No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.
(End of clause)

REC 1.7: Contractor Must Obtain Approval Prior to Engaging Subcontractors: The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.
(End of clause)

HSCEDM-17-RFI-080317

Questions and Answers

The answers provided are tentative and are for planning purposes only and the Government reserves the right to craft any eventual RFQ or SOW however we decide to, even if they contradict our answers to this RFI.

Vendor Questions	Government Response
Will ICE/ERO/TOD accept vendor services that fulfill most of the requested data, but not all (ie- FBI numbers; real time jail booking data; insurance claims; wire transfer data; incarceration data;)? As of July 1, all major credit bureaus will no longer report on individuals' public records data (tax liens, civil judgments) that have not been updated or verified within a certain period of time.	No, all data sets are mission critical, particularly criminal data.
Could you please specify what phone number account information is?	Phone numbers and related account holder information
Please specify what the required format is for the requested data.	The required format is .csv.
Does ICE/ERO/TOD want to receive alerts on the 500,000 identities daily/in real-time or monthly?	weekly and real time
What data elements will ICE/ERO/TOD provide on the 500,000 identities (name and address? SSN?) to append the requested data to?	At a minimum, we will provide full name and date of birth.
Is there an incumbent vendor for this project?	Yes
Does the Government anticipate that the subscription data services will extend past the 12 plus 6 month period?	Yes
Is this to be an ongoing resource or is it a short duration exploration of capabilities by the Government?	Ongoing resource
Is the Government looking to the Prime to host the subscription services, or will it be a capability that the Government will host in a facility of their choosing?	Prime will host the subscription services.
Does the Government have a preferred contract vehicle?	Not Yet
Is there any additional scoping information other than 500,000 identities per month?	No
What are the number of users?	4
What are the performance metrics?	Metrics depend on the demographics of the target population.
Clarify what the Government means by an in place multi-tiered vetting system.	The vendor must perform both automated and manual vetting.
How often do the source systems make available updates (event, daily, weekly...)?	Variable
What is the frequency of data change (hourly, daily, weekly)?	Overall pool changes will occur every two or three months-- unless there is a special project that needs immediate processing.
How many identity adds and deletes?	Variable amounts
What are the thresholds for the legacy system?	This question is unclear and cannot be answered.
How many false/positives and false/negatives are currently incurred and what is the most prevalent reason?	The rate is variable. Common names and identity fraud tend to cause false matches.
Does the Government have a gold data set to work with false negatives and false positive?	No
Do they have data black lists or white lists that triggers review?	No
Does the SOW represent a zero (0) degree match?	No
Does the Government want the Prime to build a graph of relationships and look at 2nd degree relationships within the corpus?	No
Is the system responsible to validate addresses and phone numbers?	Yes
What other data needs to be validated by the system?	We require overall entity resolution in addition to the validation of addresses and telephone numbers.
What commercial databases does FEDLINK, or the current subscription based service used by the TOD, aggregate data from?	CLEAR and other Thomson Reuters data services
What research support tools is the TOD currently using to support vetting?	The research support tools are to be provided by the vendor.
Does the TOD currently have access to real-time jail booking data? If so, what database is the TOD relying on for this data?	JusticeXchange
How is the data found by subscription services consumed by ICE systems?	The weekly Alert returns are stored by the government for future vetting.
Does the TOD have an estimate for the number of FTEs they want to perform this work?	All work will be performed at the contractor site. The government will not be paying directly for FTEs or determining how many FTEs are needed by the vendor.
Is there a page limit for this response?	Responses are limited to the number of output fields.
Are there formatting requirements for this response?	Required format is .csv
Where will the work be delivered?	Work will be delivered via an encrypted gateway.
What will be the government's Basis for Award?	Basis of Award has not been determined.
Is the continuous monitoring and alert system for tracking criminal aliens currently being provided? If so, which firm is providing it and what is the annual contract value and period of performance?	Yes, this service is currently being provided by Thomson Reuters Special Services, LLC.
How often or frequent are alerts expected to be generated and provided from a firm's system?	Alerts will normally be provided on a weekly basis, but results may be wanted immediately for special projects.
Is the trained analyst staffed in support of the system expected to be onsite at ICE ERO or can they be located at the firm? Are they required to be full time?	All work will be performed at the contractor site. The government will not be paying directly for FTEs and will not determine the needed number of contract employees.
The RFI states that the Government anticipates awarding a Firm Fixed Price type contract for a 12-month period of performance with a 6-month option. Is this based on RFI responses or will the Government be issuing a formal RFP in the near future? If the latter, when is an RFP anticipated to be released and will it be full and open?	Yes it is based on RFI responses. The government will be releasing an RFQ but has not made a final determination of period of performance length. At this time, the government does not know if it will be full and open or not.