DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection
Request for Information
Digital Forensic Laboratory Services

Synopsis: This is a request for information (RFI) only. This is an RFI released pursuant to FAR 15.201(e). This RFI is intended to survey the market for qualified contractors and is solely for information and planning purposes; it does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or a promise to issue an RFP or RFQ. This RFI does not commit the Government to contract for any supply or service. U.S. Customs and Border Protection (CBP) will not pay for any costs associated with responding to this RFI. All costs will be solely at the interested party's expense. While CBP intends to establish a list of qualified potential bidders, an absence of response to this RFI will not prohibit contractors from bidding on any future solicitation. The information provided in this RFI is subject to change and is not binding on the Government. All responses become the property of the Federal Government upon submission and will not be returned to vendors. CBP may elected to engage qualified vendors in one-on-one discussions prior to any future solicitation.

Purpose: This RFI seeks to gather information regarding vendor qualifications, capabilities, and past experience in the area of open source and social media analytics for market research and to establish a list of qualified bidders for future use by the agency. CBP seeks to obtain commercially and publicly available information for situational awareness tools, technologies, and methodologies able to collect and integrate diverse data sources from heterogeneous assets into a common operational picture, and deliver real-time intelligence designed for immediate human comprehension and action.

Background: CBP is one of the major components of the Department of Homeland Security (DHS) charged with protecting America's borders from terrorism, human and drug smuggling, illegal migration, and agricultural pests while simultaneously facilitating the flow of legitimate travel and trade. As the nation's single, unified border agency, CBP represents the first line of defense of America's borders. CBP agents frequently interact with the public in a variety of operational environments.

CBP's National Targeting Center (NTC) is a key component of CBP's comprehensive border security and management strategy to safeguard travelers and cargo. NTC is the point within the agency where advanced data, enterprise systems coverage, and access to law enforcement and intelligence resources is necessary to conduct vetting to identify travelers and shipments that pose the highest risk to U.S. security, economy, and public safety. Targeting traveler and cargo information plays a pivotal role of CBP's layered security strategy by extending our borders outward in order to identify and mitigate threats before they board (or are laden on) conveyances destined for the United States.

Requirements: The NTC Enterprise requires near-real time situational awareness of the global threat landscape. NTC is seeking to improve and institutionalize CBP's current open source and social media analytic capabilities by expanding the available tools and analytic techniques. Over

the course of the project, the developed tools and techniques will be formalized and, where possible, automated or otherwise incorporated into CBP systems or virtual environments. . NTC is conducting market research to determine which companies possess the necessary technology and analytical capability, have experience in delivering tools and content to Government agencies, and can provide analysis, expertise, and other technical assistance to CBP on criminal, terrorist, and foreign threats. CBP seeks to employ risk-informed approaches that incorporate intelligence, shared information, and situational awareness protocols to enable rapid response, strengthen integrated operations, and discourage future illegal activities.

Prospective contractors who are qualified to provide these services should provide the following information for CBP review:

General Information:

a. Organization Name
b. Address
c. POC (name, title, phone number, email address, etc.)
d. Business Size
e. Socio-economic status
f. Copy of GSA Schedule(s) and SINs or other GWACs (if applicable)

Questions:

1. Provide at least one, but no more than three, detailed example(s) of past performance where the contractor provided open source and social media analytical services.

2. Provide at least one, but no more than three, detailed examples of past experience providing global, near-real time situational awareness and threat assessments to Government customers.

3. Describe the capabilities, tools, and any special accreditations of your Digital Forensic Laboratory.

4. Briefly describe the range of social media platforms with which the contractor possesses the basic competencies to perform quality analytical services.

5. Describe and list the range of language competencies, to include associated confidence levels with each, accessible to your organization.

6. When outlining your capabilities, please address, at a minimum, the following activities outlined in the tables below:

Table 1: Social Media Terrorist Groups and Violent Extremist Accounts

Activity	**Details**
a. Identify potential pro-terrorist/violent extremist social media accounts.	The contractor shall monitor terrorist propaganda production and distribution, identifying corresponding social media

	accounts and forums using appropriate tools and methodologies.
b. Identify social media groups where pro-terrorist/violent extremist accounts interact	The contractor shall monitor terrorist propaganda production and distribution, identifying corresponding social media accounts and forums using appropriate tools and methodologies
c. Provide continuous feed (e.g. profiles, postings, metadata) to Government customer at mission-relevant pace.	The contractor shall be able to send relevant content to the Government customer in a manner consistent with the particular matter's relative urgency and risk.
d Develop methodology for a risk-based prioritization schema based on relevant attributes and indicators from open-source and social media content.	The contractor shall identify attributes and indicators that contribute to risk as it relates to likelihood of action, proximity of action, relative urgency, and overall potential impact.
e. Monitor reliability of risk identification process. Use results to inform attributes and indicators.	The contractor shall monitor metrics and performance measures to determine reliability of risk-based prioritization schema and adjust risk-based prioritization schema to optimize results.
f. Apply methodologies to other transnational criminal activity (e.g. human trafficking, drug trafficking, illicit trade) as directed by the Government.	The contractor may be required to expand services described in 1.a. through 1.e. to other transnational criminal activity as directed by the Government.

Table 2: Location Services (Non-GPS)

Activity	**Details**
a. Identify/Develop/Implement non-GPS methods for determining locations of pro-terrorist/violent extremist social media users.	The contractor shall apply these methods to different languages and across different regions, social media platforms, and open source forums in a repeatable process.
b. Develop and/or identify automated, repeatable process for building a "micro-localized" seed account set using computation methods. Process shall be based on both message content and social network analysis to identify other accounts that share the same micro-localization.	The Contractor shall build a working prototype tool that can be successfully used in different regions and with different languages.
	The Contractor shall develop a broader version of this technique that attempts to quickly classify the language and likely region of the account holder.
c. Apply methodologies to other transnational criminal activity (e.g. human trafficking, drug trafficking, illicit trade) as directed by the Government.	The Government may specify other domains of interest (e.g., terrorism, human trafficking, etc.) for experiments. The outputs of these efforts will be incorporated into the demonstrations, documentation, and artifact deliverables for this task.

Table 3: Persona Creation and Management

Activity	**Details**
a. Create and manage personas for gaining to online locations of interest.	The contractor may be directed to identify, create and manage personas for gaining access to platforms, sites, forums, and groups identified by the Government.
b. Create standard and repeatable methodology for persona creation and maintenance.	The contractor shall identify, develop methods, and provide training on the creation and maintenance of personas for gaining access to platforms, sites, forums, and groups identified by the Government.

Table 4: Lesser Known Social Media Communities

Activity	**Details**
a. Identify lesser known social media communities with observed terrorist or criminal communications.	The Contractor shall develop tools and methods to automate detection and gathering mechanisms for identifying the size, scope, and subject matter of online communities on other, lesser known, social media platforms, e.g., Telegram, Google+, VK, and possibly extending to other platforms such as Ask.fm and Zello.
	The Contractor shall build and maintain a catalog of these lesser known social media platforms, and provide monthly reporting on the relative status of each with regard to how often each platform is mentioned on other platforms being monitored, and potentially their perceived size, prominence, and the nature of observed terrorist or criminal communications.
	The Contractor shall develop a cost effective methodology to encompass: periodic reevaluation, continued monitoring, or escalate platforms for Government focus.
b. Evaluate/monitor emerging platforms and social media communities for a presence of terrorist and criminal activity.	The contractor may be required to develop methodologies to identify, track, and collect terrorist and/or criminal information on new platforms emerging in the social media environment.
Apply the activities from Tables 1 & 3 to additional platforms and social media communities.	The contractor may be required to apply activates from Tables 1 & 3 to platforms identified during the performance of activities a. and/or b. of Table 4.

Table 5: Transnational Organized Crime and Trafficking

Activity	**Details**
a. Develop processes (preferably automated) to identify potential social media accounts and groups owned, controlled by, or discussing organized crime groups and their activities.	The contractor shall monitor media and legal sites for information about activities, members, and related law enforcement action regarding the groups and using this information to identify corresponding Facebook accounts and forums using appropriate tools and methodologies.
	The Contractor shall develop and deliver a continuously updated list of these identified accounts and related data (e.g., postings, metadata, etc.).
b. Identify appropriate attributes and indicators to detect and/or predict relevant activities of the group.	The contractor shall identify attributes and indicators that contribute to risk as it relates to likelihood of action, proximity of action, relative urgency, and overall potential impact

Table 6: Open Source and Social Media Workshops/Working Groups/Training

Activity	**Details**
Conduct workshops and/or working groups on open source social media	The contractor may be required to conduct workshops or working groups on open source social media issues to inform the contractor's work under this project. The contractor shall coordinate facilities and participants for a successful consortium.
Conduct training on open source social media.	The contractor shall develop and execute a testing and training plan that includes performance measures and metrics. Training should be conducted as necessary or at the request of the Government.

Table 7: Open Source Analysis - Other

Activity	**Details**
a. Perform open source analysis as directed by the Government.	The contractor may be required to perform the following types of activities as part of analysis of open source content: information retrieval, text analytics, media (text and non-text) analytics, identity resolution, ontology management, geospatial, mathematics, machine learning, scalable architectures, and real time processing.

	The contractor may be required to apply foreign and domain-specific language and knowledge of culture, regions, and subjects that only an experienced human can provide.

RFI Submission Requirements

Submissions to this RFI are due to the government on Thursday, June 04 at 4:00 p.m. ET. Please send submissions by email to: NTC-RFIResponse@cbp.dhs.gov, with the email subject line: "[Vendor Name] NTC RFI Response," and copy Colin.A.Colgan@cbp.dhs.gov. Responses should be in Microsoft Word or Adobe PDF file format. When submitting your answers to the questions above, please feel free to tell us a little bit about your organization by including a capability statement, or a single electronic pamphlet, of less than 5 pages.

The Government will not publicly disclose vendor proprietary information obtained during this effort. Consistent with the Government's legal obligations, CBP will safeguard information identified by a respondent as "Proprietary" or "Confidential" to the fullest extent possible. Any information submitted by interested parties in response to this RFI may be shared by the Government with support contractors hired to assist the Government. This includes information marked as limited rights data, restricted computer software, subject to limited rights, or subject to restricted rights. The Government's support contractors that have been, or that will be hired, are required to sign non-disclosure agreements restricting them from unauthorized use and disclosure of information that may be proprietary to third party companies. By submitting information in response to this RFI, respondents are agreeing to allow the Government to share the information they submit with the Government's support contractors who are, or will be, covered by a non-disclosure agreement.

This notice is a request for information only. CBP is not obligated to release any subsequent solicitation for these services nor is it obligated to follow any of the hypothetical solicitation procedures laid out in this notice.

Point of Contact:
Name: Colin A. Colgan
Email: Colin.A.Colgan@cbp.dhs.gov