720R0000063 Social Media Solicitation

Question
Regarding "3.1.1.1 "Real time" is defined as No Later Than (NLT) one minute before incidents are reported via applicable global media sources."   What does the government consider "global media sources"? And based upon that, how does the government determine MOEs based on accuracy and relevancy?
Regarding "3.2.1. The tool shall provide alerting notifications from multiple existing social media platforms. The content of such notifications shall be derived only from publicly available, open source information." In order to provide a more accurate pricing model, can the government please be more specific regarding which social media platforms they would anticipate contractor to monitor?
Please confirm that this RFP is considered a full and open competition opportunity and that anyone may offer a bid. And that there is no preferred or recommended bidders list.
In the above referenced RFP, the following Department of Justice Acquisition Regulations: DJAR-PGD-05-08: Implementation of Homeland Security Presidential Directive (HSPD) I2 – Policy for a Common Identification Standard for Federal Employees and Contractor   DJAR-PGD-07-10: Ensuring New Acquisitions Include Common Security Configurations   DJAR-PGD-07-12: Maintaining Contractor Performance During a Pandemic or Other Emergncy   DJAR-PGD-08-04: Security Systems and Data, Including Personally Identifiable Information   DJAR-PGD-08-05: Contractor Certification of Compliance with Federal Tax Requirements   Can you please provide their full text?
How are these services currently performed (in house, contractor)? If by a contractor, please provide: a.   Contractor Name: b.   Contract #:   c.   Task Order # (if applicable):
If there is not an incumbent, what is the estimated dollar value range for this requirement?
B.4 – Anticipated Period of Performance- Please confirm the CLIN start and end dates should read May 1 through April 30th.
Contract Clauses - Can the government please provide the full text for the DJAR-PGD clauses (numbered 05-08, 07-10, 07-12, 08-04, and 08-05)?

Statement of Work- 3.1.9 – "All information provided to the FBI by the tool shall be legally obtained, and in accordance with law, regulation, policy, and applicable social media platform terms of service and privacy policies." As the government may know, certain social media companies require that an Offeror's Social Media Alerting solution using the social media company's data must include specific product modifications and safeguards prior to that solution being sold to the government.
SF 1449 Document- Please confirm the SF 1449, cover page, table of contents and any representations and certifications are exempt from page count.
SF 1449 Document- Please confirm an Offeror's representations and certifications should only be filled out in SAM as detailed in the RFP, Section K.
Section L, Format and Font Size – Are offerors bound to a minimum font size, and if so, can graphics and tables use smaller or larger font sizes?
Section L, Page Count – Confirm page count is final. Does specified RFP page counts include table of content and cover pages?
General – Is there currently an incumbent? If so, please provide vendors name and contract award number.
Social Media Platforms – Are there specific social media platforms and/or data feeds the FBI is requesting?
General – In the vast areas of the world where social media is not a relevant or primary source of communication will the FBI accept the use of other forms of alerting data?
Attachment 2 SOW page 2: "3.1.1.1 "Real time" is defined as No Later Than (NLT) one minute before incidents are reported via applicable global media sources. Not all incidents are reported first by social media. How is this to be measured? https://www.forbes.com/sites/kalevleetaru/2019/02/26/is-twitter-really-faster-than-thenews/#2ac948cf1cf7
Attachment 2 SOW page 2: "3.1.3 Alerts provided shall be vetted by the contractor for accuracy and relevancy before they are provided to the end user." is machine vetting acceptable for this requirement? What error rate is acceptable?
Attachment 2 SOW page 3: "3.1.4 The tool must allow for review of notifications before such information can be saved to FBI systems." How would notifications be saved to FBI systems? If the system sends an email, it needs to be received by FBI email before the notification can be reviewed.
Attachment 2 SOW page 3: 3.1.7 Under what circumstances would a tool automatically download to an FBI system of record?

Attachment 2 SOW page 3: "3.1.8 The tool should not retain information, or if it does retain information, it must self-purge such information every 7-10 days." What constitutes information in this context? May the tool retain publicly available information for all customers to allow for historical searches of data as described in 3.3.3.2 "The tool shall also permit the end user to seek relevant historical publicly available data from social media platforms for further analysis."? If users define queries for which they wish to be alerted, is the maximum time those queries are allowed to be stored 10 days? Are user accounts to be deleted within 10 days?
Does this solicitation create a follow-on contract related to DJF171200P0002894, or is it a new effort or program? If it is a new effort or program, how will it function or relate to contract DJF171200P0002894?
What is the relationship between this solicitation and solicitation #DJF194750PR0000369?
Is there an incumbent(s) that provide the required capabilities? If there is an incumbent, how many users were stated as a requirement in the incumbent contract/SOW? How many users are currently using the solution?
Does this solicitation represent a consolidation effort on behalf of the government to procure a single tool to replace many? If so, how many tools is the single selected solution replacing?
Will the government further define events/activities within the "National Security" and "Public Safety" categories, or is the vendor expected to provide these sub categories of events/activities?
Using the definition of accuracy in 3.1.3.1, it seems likely that no tool will be compliant as 100% accuracy using publicly available information is not achievable. Therefore, for SOW Section 3.1.3, would the government be open to modifying the definition of accuracy based on the successful contractor's technical approach to mitigate inaccurate information prevalent in publicly available data? Would the government be open to adding accuracy as an evaluation criteria or adding a commercially reasonable efforts standard?
With respect to Section 3.1.8 for self-purging information, is there a scenario whereby a user has flagged a particular alert and may require future access to that alert beyond a 7-10 day period?
Section 3.3.3.1 – Can the government define the requested feature called "photographic tagging"?
Section 3.3.3.2 – is the requirement for permitting end users to create filters for alerts specific to the user's mission, akin to the user only receiving a subset of alerts in specific events/activities?
Regarding Section 3.4 of the RFP, for users accessing the selected solution on a desktop computer, will users access the solution via the standard unclassified government network, or via some other means?
Section 3.5.2: What are the steps to completion, and the anticipated timeframe, associated with the FBI Security Risk Assessment?
Is a facility clearance required?
Does the successful bidder need to be a US company?

Within Technical Factors, are all sub-factors equal in weight? If not, would the government provide the relative weighting between the Technical sub-factors?
Will a vendor's compliance practices around social media terms and conditions, be a consideration in the governments evaluation of tools?
Will the Government consider a vendor's ability to implement granular security controls to limit use of tool features based on a user's role or other attributes, as well as the ability to audit end-user use of the tool to ensure end-users abide by the Government's acceptable use standards?
With respect to Part IV instructions, will the government accept a PDF submission?
In acknowledgment of the requirement that the apparent awardee will be required to provide an oral presentation and demonstration of its tool which will be evaluated for compliance with the listed laws and standards, including the Privacy Act, 5 U.S.C. 552a, will the government consider its employees' user accounts on the selected platform to meet the definition of a "system of records" under the Privacy Act? If so, can the government confirm that the requirements of 552a(m) would then apply to the apparent awardee?
The solicitation incorporates FAR 52.227-19, a non-mandatory clause that grants the Government greater rights in commercial computer software than normally would be granted in a commercial license. Because the granting of these additional rights in offerors' commercial software likely will result in increased prices to the Government, and because it is likely that the Government's needs can be fulfilled through a standard commercial license, please confirm the incorporation of FAR 52.227-19 is necessary here, or whether the government would consider removing?
The solicitation and accompanying SOW frequently reference social media and social media platforms. However, national security and public safety interest related content is found in many other locations of the internet that may not be referred to as "social media." Would the offeror receive additional credit for providing the ability to receive publicly available information regardless of origin on the internet?
Is the governments intent with the definition of "real time" to exclude potentially valuable content related to national security or public safety incidents from publicly available data sources that do not support high volume or frequency API connections, aren't referred to as social media or don't themselves update in real time?
Is this RFP related to FBI's RFI request for Media Analytic Capability in April 2019 which came out of the FBI Office of Public Affairs?
Which social networks will be analyzed? (E.g. Facebook, Twitter, etc.)

Will any other data sources other than social media networks need to be analyzed?
Is the expectation that the FBI will enter into the required social media or other data source agreements required for analytics?
What is the expectation surrounding the requirement for historical publicly available data from social media platform? Is the requirement that the service provider be able to access and provider data beyond a certain time frame?
What is the geographical scope of the analyses to be conducted (e.g. will only US social media accounts be assessed, or is the scope broader than the US)?
What are the expectations surrounding geo-tracking / geo-fencing? Is there an expectation that geolocation data will be provided?
Will monitoring of individuals and identification of social media users be required?
What are the expectations surrounding the requirement that the contractor "vet accuracy and relevancy" before providing results to the end user? What will this "vetting" entail and how should this be conducted?
What is the expectation surrounding "photographic tagging"? Will there be a requirement to tag specific locations, objects, individuals, etc.? Is there any expectation to provide facial recognition data?
With respect to the 2-hour cyber security breach notification requirement, how will a "breach" be defined?
The requirement is to provided notification within 2-hours of "discovery": how will "discovery" be defined (for e.g. after a conclusion has been drawn, or where there is a mere suspicion of a breach that has yet to be confirmed)?
What will the FBI security risk assessment entail?
What is the anticipated interplay between the requirement to "vet" and the requirement to provide "real time" alerts? If the required vetting delays an alert beyond the "real time" standard, how will this be handled?

What are the "applicable global media sources" for purposes of establishing the real time standard?
Will additional guidance be provided to the contractor about events considered to be "national security incidents," which is a potentially subjective term?
Is this effort being coordinated with the National Threat Operations Center? Is the NTOC a receiver of this information?
Is this is a re-compete or a consolidation of tools? I was wondering how it might pertain to our current contract.
Does this cover all platforms or only certain ones?
What is the total number of users the FBI expects to deploy the solution to?
Can you clarify/define "content" vs. "category" in the types of segments?
Do all the parts of the solution need to be from an American company or can you partner with others?
What are the list of preferred social media sites you want monitored? Will it expand over time?
What is the number of physical assets/locations you want tracked?
Is the solution meant to be hosted on-premise where FBI stores all the data, or is the solution meant to be SaaS-based where the provider hosts the data?
If SaaS-based and hosted by the provider, what is the estimated query limit per day?
How many end users will be using the solution?

Should the offeror's firm-fixed price also include custom software develop for the COTS solution?

Government Response
The RFT is for an alert capability. From a definition stand point, real time means "in real time". The purpose of this RFP is to provide the FBI with notification so that first responders and law enforcement can respond as quickly as possible to potential chances that an accurate and appropriate response can be initiated. The intent would be to cover the largest geographical regions possible. Language algorithms should ensure the information provided has been translated correctly. While a margin of error (MOE) is likely, the vendor should ensure a comprehensive vetting process is maintained. The MOE should remain less than one percent.
There is not a specific site or sites. The development and design of the tool is the onus of the vendor. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes. Vendor's are encouraged to provide the most comprehensive data sets available in order to provide first responders and law enforcement officials with timely, relevant and accurate notifications.
This requirement will be competed as full and open, there is no "preferred or recommended" bidders list.
See second Tab of this spreadsheet titled "DJAR Local Clauses"
Contractor Name: Dataminr, Inc. Contract #: DJF-17-1200-P-0002894 Task Order # (if applicable): N/A
There is an incumbent, the government has an Independent Government Cost Estimate, but proposals shall be provided independent from that information.
Period of performance for each CLIN will be – May 1 through April 30th., following the years indicated in section B.4.
Answered in Question #2.

The successful bidder is responsible for ensuring their product meets the requirements for privacy and civil liberties compliance protections.
The page numbers should start after the table of contents.
Correct, current and accurate data must be registered in Sam.gov.
All font size should be 12-point font.
The page count is final and specifics to page numbering is answered in Question #10.
This is answered in Question #5.
There is not a specific site or sites. The development and design of the tool is the onus of the vendor. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes. Vendor's are encouraged to provide the most comprehensive data sets available in order to provide first responders and law enforcement officials with timely, relevant and accurate notifications.
The FBI does not want to identify the sources from which the data is provided. The vendor should delineate those selections and provide the most accurate and timely data possible.
The RFP is for an alert capability. From a definition stand point, real time means "in real time". The purpose of this RFP is to provide the FBI with notification so that first responders and law enforcement can respond as quickly as possible to potential chances that an accurate and appropriate response can be initiated.
It is the responsibility of the vendor to determine their own internal vetting processes. While a margin of error (MOE) is likely, the vendor should ensure a comprehensive vetting process is maintained. The MOE should remain less than one percent.
The FBI is not seeking to save information from the notifications but rather use it to ensure timely response to incidents around the globe, of importance to the FBI. This feature should be similar to an RSS feed or other news altering capability.
The intent of this product is for the vendor to provide the FBI with advanced notification of incidents around the globe that may be of interest to the FBI. In many cases, our employees are mobile. Notifications should be easy to obtain and relay.

The vendor has the discretion to determine what they wish to store on their own platforms. The FBI is looking for instant notifications. The information decreases in value as it ages; therefore, we are not looking for long term repositories of information, but rather quick, immediate updates on situations that are occurring in real time. The intent is not to delete user accounts but to not compile old notifications.

Contract DJF171200P0002894 is the current contract that is expiring. This RFP is for the re-compete of that effort.

The scope of work has been re-evaluated and more defined since that time. 15F06720R0000063 now replaces DJF-19-4750-PR-0000369.

The FBI does not comment on current capabilities.

Please refer to Section B.1 on page 4 of the RFP.

This RFP is for an alerting capability. Keywords should be derived by the successful bidder and determine the appropriate algorithms to provide the FBI with mission and national security relevant information.

It is the responsibility of the vendor to determine their own internal vetting processes. While a margin of error (MOE) is likely, the vendor should ensure a comprehensive vetting process is maintained. The MOE should remain less than one percent.

No. Information decreases in value as it ages. The intent of this tool is for immediate updates and can be deleted after they are provided.

Many social media platforms provide the ability to tag a photograph with a name or other descriptor. The government is simply referring to that functionality.

This RFP is for an alerting capability. Keywords should be derived by the successful bidder and determine the appropriate algorithms to provide the FBI with mission and national security relevant information.

The end user will access the solution via the unclassified network as delineated in the RFP.

The contractor will be expected to meet all of the security requirements outlined in the RFP. Please see Section 2 Background for the parameters of who will have access to the data.

No

No. However the successful bidder must have all proper clearances.

While each evaluation factor is important, the alerting capability is the most significant. The subsequent factors decrease in importance in the order they are listed in the RFP.
While each evaluation factor is important, the alerting capability is the most significant. The subsequent factors decrease in importance in the order they are listed in the RFP.
While each evaluation factor is important, the alerting capability is the most significant. The subsequent factors decrease in importance in the order they are listed in the RFP.
Yes. Adobe PDF is acceptable however all documents sumbitted must be searchable.
It is the successful bidder's responsibility to ensure they comply with all legal requirements. The FBI expects that all vendors will comply with all privacy and civil liberties statutes including but not limited to the Privacy Act, Title 5 of the U.S. Code, Section 552A, as well as any applicable rules, policies, and regulations set by the agency, government, and/or owner of the social media platforms.
FAR 52.227-19 has been removed from this solicitation.
The FBI does not want to identify the sources from which the data is provided. The vendor should delineate those selections and provide the most accurate and timely data possible. While each evaluation factor is important, the alerting capability is the most significant. The subsequent factors decrease in importance in the order they are listed in the RFP.
There is not a specific site's, the development and design of the tool is the onus of the vendor. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes. Vendor's are encouraged to provide the most comprehensive data sets available in order to provide first responders and law enforcement officials with timely, relevant and accurate notifications.
No.All proposal submissions for should pertain to the requirements of this SOW ONLY.
There is not a specific site's, the development and design of the tool is the onus of the vendor. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes. Vendor's are encouraged to provide the most comprehensive data sets available in order to provide first responders and law enforcement officials with timely, relevant and accurate notifications.

There is not a specific site's, the development and design of the tool is the onus of the vendor. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes. Vendor's are encouraged to provide the most comprehensive data sets available in order to provide first responders and law enforcement officials with timely, relevant and accurate notifications.

As defined in Section 3.3.3.2 Alerting, the SOW is requesting advanced modifications of mission-relevant incidents. Data should be provided quickly but then does not have to be stored or maintained for future purposes, as this tools is only meant to provide notifications.

The intent would be t cover the largest geographical regions possible. Language algorithms should ensure the information provided has been translated correctly.

Yes. The location of an incident is critical to identifying that a situation is occurring. The most comprehensive notification system would ideally identify where a disturbance, incident or other event of interest may be occurring at any given moment.

No. At no time will this tool be used to identify private citizens. This tool is solely meant to be used as an advanced notification of events occurring.

It is the responsibility of the vendor to determine their own internal vetting processes. While a margin of error (MOE) is likely, the vendor should ensure a comprehensive vetting process is maintained. The MOE should remain less than one percent.

Is there any expectation to provide facial recognition data? The purpose of this tool is to provide the most informative information surrounding an event that is unfolding. Phototagging is useful when trying to identify an area where an event may occur; however, it is not the only criteria that will be considered. The government is interested in the most comprehensive, yet accurate notifications of worldwide events.

The requirement to notify the FBI of any potential or actual computer security incident would apply to any party responsible for providing the requested services to the FBI, contractor or sub-contractor alike.

All input and output of capability to ensure laws, policies, and regulations concerning any private information are followed. In the event that a breach should occur, the vendor must have security measures and protocols in place to follow through with properly informing the FBI, containing and mitigating the situation.

This is answered in Question #32.

The intent would be to cover the largest geographical regions possible. Language algorithms should ensure the information provided has been translated correctly. While a margin of error (MOE) is likely, the vendor should ensure a comprehensive vetting process is maintained. The MOE should remain less than one percent.

The RFT is for an alert capability. From a definition stand point, real time means "in real time". The purpose of this RFP is to provide the FBI with notification so that first responders and law enforcement can respond as quickly as possible to potential chances that an accurate and appropriate response can be initiated.
This RFP is for an alerting capability. Keywords should be derived by the successful bidder and determine the appropriate algorithms to provide the FBI with mission and national security relevant information.
No. It is not. This information is requested for the FBI's use.
This is answered in Question #22.
This RFP requests real time notifications of events that could be of importance to the FBI. The platforms used by the vendors are solely at their discretion. The FBI does not have a preferred platform; instead, we are most interested in the accuracy and comprehensive nature of the data provided.
No. Usage is based on the number of individuals with that mission focus. While a specific number is not available and would vary based on licensure types and requirements, an estimated user population would be between 1,000-2,000 individual users.
The government does not understand the question. The request is for notifications of events in near to real-time. The type of event can be described in a manner the vendor feels is appropriate. The government does not wish to categorize the events in a specific manner; however, they should be organized and easy to quickly search.
All offerors must be registered on Sam.Gov prior to the close date of solicitation to be eligible for award. The company have the appropriate clearance levels to bid on contracts of this nature.
No, there currently is not a list of sources, sites or digital locations that must be included in the solution's capability. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes.
No, there currently is not a list of sources, sites or digital locations that must be included in the solution's capability. The FBI's requirement is not for one specific social media platform versus another, but rather for the most comprehensive, accurate and relevant information available for immediate alerting purposes.
Existing systems are not of relevance to this request. This product should be a standalone product that provides alerts
The development of sourcing, and the resulting capability, is the responsibility of the vendor. It is the responsibility of the vendor to utilize metrics that conform with all relevant laws and statutes while providing an alerting capability. The FBI cannot provide specific attributions or non-attributions that the vendor should include in its query metrics for the vendor's platform.
No. Usage is based on the number of individuals with that mission focus. While a specific number is not available and would vary based on licensure types and requirements, an estimated user population would be between 1,000-2,000 individual users.

Please see the response to question 69. This request is for an alerting capability. The specific system development and functionality are the responsibility of the vendor.