

**Public Source Program Office  
for the  
Office of the Chief Information Officer**



**Social Media Alerting  
Statement of Objectives**

**Request for Proposal  
Number  
DJF194750PR0000369**

**07/8/2019**



# FEDERAL BUREAU OF INVESTIGATION

## Social Media Alerting

### Statement of Objectives – ATTACHMENT TWO



## 1 Scope

This Statement of Objectives (SOO) describes the Federal Bureau of Investigation's (FBI, or "the Bureau") requirements to proactively identify and reactively monitor threats to U.S. National interests, through means of online sources.

## 2 Background

The Public Source Program Office (PSPO) is a group within the Enterprise License Agreement Management Unit of the Office of the Chief Information Officer, which manages public records contracts, facilitates training and establishes guidelines for usage and account management.

This PSPO's public records contract is in response to an increasing number of threats to U.S. national interests that are identifiable, with ever-greater frequency, through social media platforms. It is an acknowledged fact that virtually every incident and subject of FBI investigative interest has a presence online. Consequently, law enforcement gaining lawful access (i.e., access that is authorized, appropriate, and consistent with applicable law and policy) to this data will result in early detection and/or containment of the magnitude of any harm caused by these threats.

To protect US citizens, a method employed by the FBI is the acquisition of subscriptions granting access to tools. These allow for the exploitation of lawfully collected/acquired from social media platforms and stored, vetted and formatted by a vendor. The mission-critical exploitation of social media enables the Bureau to proactively detect, disrupt, and investigate an ever growing diverse range of threats. More specifically, the Bureau provides real-time situational awareness of indicators and warnings of emerging social media incidents.

All FBI Headquarters Divisions and Field Office personnel (government and support contractor) may receive the benefit of the information that is produced under the instant procurement action, should they require access to relevant data as part of their duties and responsibilities.

The need for social media, although identified as Enterprise wide in terms of location, stems from specific groups of users. Within each division and field office, users from various career paths are set on a Social Media Exploitation mission to address a broad range of threats. Specific mission groups that call for such a capability include the following:

Operations centers and watch floors. These are the groups within the Headquarters and Field Offices that ensure news and events are identified, vetted and swiftly reported to the appropriate action group. The functions of most value by these individuals is early notification, accuracy of information, and the ease by which information is disseminated.



# FEDERAL BUREAU OF INVESTIGATION

## Social Media Alerting

### Statement of Objectives – ATTACHMENT TWO



Fusion centers. Operations-driven tactical teams that are deployed as soon as an incident is validated by the Operations center. The functions of most value by these individuals is early notification, the provision of accurate geo-locations, and the mobility of the needed capability.

Legal attaches. FBI personnel are deployed internationally and sometimes in areas of press censorship. A social media exploitation tool with international reach and paired with a strong language translation capability, can become crucial to their operations and more importantly their safety. The functions of most value to these individuals is early notification, broad international reach, instant translation, and the mobility of the needed capability.

Command posts. These are teams composed of power users assigned to the proactive monitoring of large events in a preventive stance, or deployed to a theatre of operations in a reactive stance. The function of most value to these individuals is multi-layered geo-fencing, strong analytical and prioritization algorithms, and analysis with historical data accessibility.

#### 2.1 Accessibility

Bureau personnel and their authorized support-contractor personnel shall be able to gain access to the required information via web browser and through multiple devices, to include desktop and FBI-issued mobile devices hosting contractor-maintained applications downloaded onto the FBI device. Some mobile devices will require the download of an application. The latter can only be made available after thorough vetting by the Mobility program. **The offer must include a technical a description, in the form of a Contractor Statement of Work (CSOW) to allow for initial assessment and evaluation of compatibility.**

### 3 Objectives

#### 3.1 Program Objective

The objective of the PSPO is to centralize the acquisition of subscriptions services to a social media early alerting tool in order to mitigate multifaceted threats, while ensuring all privacy and civil liberties compliance requirements are met.

#### 3.2 Contract Objective

The objective of this procurement-action is to acquire access to the data needed for the FBI to conduct social-media-alerting and related analysis.

#### 3.3 Functional Objectives

Delineated below are the expected Outcomes (Critical Success Factors) to be achieved by the Contractor, along with associated Standards by which the Contractor is to abide when delivering the Outcomes (Key Performance Indicators) relative to the Government's access to a social-media-alerting and analysis tool.



**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



The Standard applicable to the achievement of any and all Objectives is that any information obtained and made available to the Government is lawfully obtained.

### **3.3.1 Alerting**

*3.3.1.1 Outcome: The FBI receives advanced notifications of mission-relevant incidents.*

#### **3.3.1.2 Standards**

3.3.1.2.1 Information constituting advanced notification is derived from constant monitoring of social media platforms based on keywords relevant to national security and location.

3.3.1.2.2 Notifications are sent via email to either a team account or individual user accounts based on real time threat, incidents as they tie to the geolocation of interest. Selected tool must allow for customization of delivery frequency, content of interest and geographical layers by the user directly.

3.3.1.2.3 Content filtering supports prioritization; specific subjects, identifiers, geographic location, keywords, photographic tagging.

3.3.1.2.4 Users are able to select to monitor the development of a notification-of-interest, as well as seek relevant historical social media traffic for further analysis.

CONTINUED ON NEXT PAGE



# FEDERAL BUREAU OF INVESTIGATION

## Social Media Alerting

### Statement of Objectives – ATTACHMENT TWO



#### 3.3.2 Analysis, display and sourcing

3.3.2.1 *Objective: The FBI accesses historic data to identify profiles and ramifications to derogatory groups.*

3.3.2.2 *Standards:*

3.3.2.2.1 Obtain the full social media profile of persons-of-interest and their affiliation to any organization or groups through the corroboration of multiple social media sources.

3.3.2.2.2 Items of interest in this context are social networks, user IDs, emails, IP addresses and telephone numbers, along with likely additional account with similar IDs or aliases.

3.3.2.2.3 Any connectivity between aliases and their relationship must be identifiable through active link analysis mapping.

3.3.2.2.4 The analytical mapping process is depicted through active links between visual data points (e.g., not just showing two entities are connected, but showing key items of connection when hovering over the link).

3.3.2.2.5 The data presented must be reliable, accurate and consistent.

3.3.2.2.6 Users can perform individual queries, as well multiple queries at once through batching by uploading a spreadsheet of identifiers at once. Individual query process is not automated and requires user input of a single or multiple search criterion.

#### 3.3.3 Geo Location, keywords and timeframe

3.3.3.1 *Objective: The FBI exploits data in a real-time context, in both a proactive and reactive stance, based on location.*

3.3.3.2 *Standards*

3.3.3.2.1 Online media is monitored based on location, determined by the users' delineation or the import of overlays from existing maps (neighborhood, city, county, state or country). These must allow for customization as AOR sometimes cross state or county lines.

3.3.3.2.2 Traffic on area types described in 3.3.3.2.1 is filterable and customizable by keywords related to special or significant identifiers (keywords, usernames, handles).

3.3.3.2.3 Geolocation and keywords presented in 3.3.3.2.1, 3.3.3.2.2 allow for specific timeframe query with start and end fields that can be populated with date and time. This allows for monitoring and filtering directly after or as the significant event develops.

#### 3.3.4 Security

3.3.4.1 *Objective: The FBI receives immediate notification and support by the contractor for any possible computer security breach incidents exposing FBI information.*

3.3.4.2 *Standards*



**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



3.3.4.2.1 The FBI is notified of possible, potential and currently occurring incidents impacting the vendor's interface.

3.3.4.2.2 The Contractor provides the FBI with technical points of contact and supporting technical documentation (i.e., systems configurations, related security files, contingency plan and recovery process) with its notification as well as the assessed magnitude of FBI user information exposed.

### 3.3.5 Queries

3.3.5.1 *Objective: Any information inputted or provided by FBI personnel for input into the vendor's interface remains protected.*

#### 3.3.5.2 Standards

3.3.5.2.1 Searches conducted on the Contractor's interface by FBI personnel remain untraceable under Blind Login.

3.3.5.2.2 Entries, activities such as saved searches and links activated remain untraceable and cannot be stored by the offeror or used to create alert profiles presented or used by other agencies, without the FBI's consent.

3.3.5.2.3 Searches remain non-attributable.

### 3.3.6 Reporting

3.3.6.1 *Objective: The FBI is informed of any potential or actual computer security incidents involving or potentially involving FBI information or users.*

#### 3.3.6.2 Standards

3.3.6.2.1 The FBI is informed of any potential or actual computer security incidents as soon as the Contractor becomes aware of the issue. The Contractor notifies the FBI immediately in the event of a breach of FBI information involving personally identifiable information of FBI personnel (e.g. First and/or last name, email, phone number, location).

3.3.6.2.2 Logging of FBI personnel queries are limited to the collection of numeric metrics for usage monitoring (Occasionally, the FBI may require data logging for the purposes of internal investigations, testing, debugging or usage monitoring. This will only be done through the explicit written permission of the FBI and with specific limitations).

### 3.3.7 Training and Testing

3.3.7.1 *Outcome: FBI personnel receive training on the Contractor's related tools and techniques.*

#### 3.3.7.2 Standards

3.3.7.2.1 Holders of newly created accounts receive initial training when first gaining access credentials to the Contractor's tool.



**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



3.3.7.2.2 Refresher trainings is provided whenever a new release of the Contractor's tool is released.

3.3.7.2.3 Material conveying changes and/or enhancements are made available to each user.

3.3.7.2.4 Training material is accessible via the Contractor's interface and/or video-sharing platform, in compliance with standards set forth in Section 508 of the Rehabilitation Act of 1973.

3.3.7.2.5 For written online material, soft copies undergo review and obtain validation after each major release.

3.3.7.2.6 Two one-hour monthly online training sessions are made available for each user.

3.3.7.2.7 One of the monthly training sessions is directed to new users and introduce the capability, where to find resources, basic trouble shooting steps, helpdesk structure, and POCs.

3.3.7.2.8 The second monthly training session is focused on new features, system upgrades, and best practices derived from usage.

3.3.7.2.9 A course outline is provided to the PSPO Training Coordinator for review and approval prior to dissemination.

### **3.3.8 Helpdesk**

*3.3.8.1 Outcomes: FBI personnel with access or other issues obtain support from designated helpdesk personnel.*

*3.3.8.2 Standards*

3.3.8.2.1 Designated helpdesk personnel are familiar with the sensitivities of government and law enforcement.

3.3.8.2.2 A specific email address is established and maintained for FBI personnel and authorized support contractor personnel to seek assistance.

3.3.8.2.3 Requests for helpdesk assistance are acknowledged within 60 minutes.

3.3.8.2.4 Helpdesk personnel adequately protect the confidentiality of inquiries by users.

3.3.8.2.5 Helpdesk personnel adequately ensure the legitimacy of the call recipient.





**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



#### **4 Contract POCs**

For daily operations the PSPO will be the direct counterpart to the Contractor's management personnel and will provide guidelines for communication. Announcements and general notifications will be conveyed to users through the PSPO, unless the selected offeror is responding to a direct helpdesk inquiry.

No communication pertaining to new capabilities, business development, surveys or contract notification are to be addressed by the Contractor directly to the users, without the approval of coordination of the PSPO staff.

##### **4.1 Contracting Officer (CO)**

The CO is the appointed authority to bind the Government to the extent of the authority delegated. Direction that will modify the scope, schedule, terms and conditions, funding, or any other action that may modify the agreement, as originally entered into with the Government, must be given only by the CO.

Name: Garland Crosby

Title: Contracting Officer

Phone: (202) 324-9013

E-mail address: [GLCrosby@fbi.gov](mailto:GLCrosby@fbi.gov)

##### **4.2 Contracting Officer Representative**

The COR will be identified via letter of COR delegation authority issued by the Contracting Officer (CO) for this contract. The COR is responsible, as applicable, for: receiving all deliverables; inspecting and accepting the supplies or services provided hereunder, in accordance with the terms and conditions of this contract; providing direction to the Contractor which clarifies the contract effort, filling in details or otherwise furnishing information necessary to accomplish the SOW; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment. The COR does not have the authority to alter or modify the Contractor's obligations, contract terms, conditions, specifications, or cost. If as a result of technical discussions, it is in the Government's best interest to alter/change contractual obligations or the SOW, the CO will issue such changes:

Name: **TO BE ANNOUNCED AT THE TIME OF AWARD**

Title:

Phone:

E-mail address: [j](#)

##### **4.3 Program Manager**

The program manager is responsible for all day-to-day operations of the program, as well as maintaining its history for auditing purposes, and defining the way ahead that will ensure full exploitation of the acquired capabilities. The program manager will establish and coordinate the quality control, training deployment, and user account administration as his/her team will serve as the liaison between the offerors and the end users. The





**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



program manager will coordinate, attend, and report on the mandatory monthly meetings held with awarded offerors.

Name: **TO BE ANNOUNCED AT THE TIME OF AWARD**

Title:

Phone:

E-mail address:

**5 User account management**

Access to public records data must remain within the investigative confines, and therefore, must be internally closely monitored. The offeror must provide account and username management. Since users span across all Field offices and Resident Agencies (RAs) as well as HQ Divisions, the monitoring of accounts along with usage will require different levels of administrative rights.



**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



*5.1 Public Source Program Office Administrative accounts*

**5.1.1 Structure**

*5.1.1.1 Outcome: Autonomous user administration by the FBI*

*5.1.1.2 Standard*

5.1.1.2.1 Social Media SMEs are present within each Field Office and division and serve as local user administrators. Administrative rights accounts allow for local creation, maintenance and deletion of user accounts within their respective Field Offices and HQ Divisions.

5.1.1.2.2 Administering their local users is a collateral function as these SMEs are heavily embedded in their area of mission expertise. Therefore they need system as well as administrative access rights.

5.1.1.2.3 At the Program level, Super Admin accounts allow for the creation, maintenance and deletion of the administrative accounts described in 5.1.1.2.1. Super administrative accounts do not require system access or user view as their purpose is solely administrative.

*5.2 Monitoring and reporting*

**5.2.1 Reports**

*5.2.1.1 Outcome: The FBI must be able to monitor usage to assess the operational value gained from the capability.*

*5.2.1.2 Standard:*

5.2.1.2.1 Monthly reports are received by the 10th of each month.

5.2.1.2.2 These monthly reports are distributed via email to the aforementioned FBI Contracting Officer and Contracting Officer's Representative (COR). Any additional recipient must be approved by the COR.

5.2.1.2.3 Monthly reports are delivered in an excel file format. The monthly report includes all the below:

- Activities, Accomplishments, and Issues reports
- Monthly Summary and Detailed Usage reports (metrics only, no content)
  - individual account
  - team account
  - batching
- Monthly Account Listing reports broken down by field office
  - New accounts
  - Deleted accounts
  - Transferred accounts
- Completed training sessions broken down by locations, subject and list of attendees



**FEDERAL BUREAU OF INVESTIGATION**  
**Social Media Alerting**  
**Statement of Objectives – ATTACHMENT TWO**



### 5.2.2 Monthly Meeting

5.2.2.1 *Outcome: The purpose of these meetings is to review the monthly activities presented in the monthly report, address any issues reported to the program and monitor the contract progress.*

5.2.2.2 *Standard:*

5.2.2.2.1 Meetings occur every month and can be held via conference call, but occur in person at least once every quarter with the COR/PM in attendance.

The standard agenda is below but can be modified as needed

- **Contract**
  - o Invoice status
- **Reports**
  - o Usage (Previous Month and Current Fiscal year to date)
  - o Account maintenance activity
- **Training**
  - o Completed trainings to date (current FY)
  - o Upcoming trainings
- **System upgrades/changes**
  - o Release notes
  - o Impact on users
- **Vendor's new capabilities and recommendations**
  - o Presentation
  - o Pricing model (license/account/usage)

## 6 Release of information

The FBI specifically requires that Contractors shall not exploit for interface development, disclose information or produce material acquired as a result of, or derived from operational activities of FBI personnel on their interface.

For purposes of this Clause, "Information" shall include, but is not limited to: in any media or all media including on the web or websites, publications, studies, books, theses, photographs, films or public announcements, press releases, describing any part of the subject matter of this contract or any phase of any program hereunder, except to the extent such is:

- (i) Already known to the Contractor prior to the commencement of the contract.
- (ii) Required by law, regulation, subpoena or government or judicial order to be disclosed, including the Freedom of Information Act.

No release of information shall be made without the prior written consent of the Office of Public Affairs and the Contracting Officer. The contractor and author are warned that disclosure is not without potential consequences. The FBI will make every effort to review proposed publications in a timely manner to accommodate these and other publications. These obligations do not cease upon completion of the contract.