Statement of Work (SOW)
for
Software-as-a-Service (SaaS) Solution for
Social Media Research Services for

The United States Army
Criminal Investigation Division

25 March 2020

PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATION OR DISTRIBUTION OF THESE DRAWINGS, PLANS OR SPECIFICATIONS TO UNAUTHROIZED USERS IS PROHIBITED

PROPERLY DESTROY DOCUMENTS WHEN NO LONGER NEEDED

DO NOT REMOVE THIS NOTICE

1.0 BACKGROUND:

The United States Army Criminal Investigation Command (CID) mission is to investigate all felony crimes related to or of interest to the U.S. Army. As the primary investigation organization within the U.S. Army, their mission is focused on the following: serious crime; sensitive and/or serious investigations; collection, analysis and dissemination of criminal intelligence; protective service operations; forensic laboratory support; maintenance of Army criminal records; force protection support and logistics security.

2.0 REQUIREMENTS:

The CID has a requirement for 13 Subscription Services for annual web based service that shall provide reliable social media research services, also referred to as a Software-as-a-Service (SaaS) solution. These software licenses are required for use in criminal investigations and other missions conducted by the CID. This SaaS solution shall provide a secure and legal social media threat detection and risk mitigation. The SaaS solution shall be web based with subscription service to support organizations' ability to quickly unlock the value of social media and big data to assess risk, respond to threats, and discover actionable intelligence.

Administration of the service will be done from Headquarters, USACIDC, Quantico, VA, with users located throughout the U.S. and overseas where there is a USACIDC presence.

Training will be provided on-site at designated CID HQ locations at Quantico, VA; Hunter Army Air Field, GA; and Joint Base Lewis-McChord, WA.

The period of performance is for three years, consisting of a 12-month Base Period and two (2) twelve 12-month Option Periods for annual subscription service and training.

3.0 DESCRIPTION OF SUPPLIES:

Contractor shall provide software that meets or exceeds the following specifications:

3.1 - 13 Subscription Services:

-The SaaS shall be web based subscription service. Vendor provided software client may be utilized to access the service. No hardware to install.

-The service shall have the capability for the customer administrators to establish user accounts and set user permissions (role-based controls). The administrators shall also have the ability to conduct audits of users search histories and current collection efforts.

Technical Acceptability Criteria:
-The SaaS must be web based. No hardware or software to install.

-The capability/solution shall be a fully functional COTS capability and ready to begin to accept and enroll user profiles and enable required feature/function one (1) day after the contract is awarded.

-The capability/solution must have the ability to provide real-time threat intelligence feed utilizing a mixture of human and automated security operations, and capable of harvesting intelligence from at least 70 web based platforms, to include all international platforms, both open and closed sources (Deep and DarkWeb), social media sites (Facebook, Twitter, LinkedIn, Instagram, YouTube, VK, etc.), Blogs, Images and Videos, and capable of expanding to other advanced web based data sources.

- The capability/solution shall be responsible for any agreements with the required social media organizations that will enable the capability to execute and perform successfully, that are in line with the platform Terms of Service (ToS) agreements.

- The capability/solution must be able to deliver actionable intelligence in a timely manner by providing alerts in real-time, normalizes data feeds (remove duplicates, enables user-set rules, etc.), integrates with SIEM, firewall logs, etc., uses natural language processing (NLP) to ensure threat actor chatter on hidden foreign-language forums is identified, and uses Artificial Intelligence (machine learning and predictive analytics). This broad range of inputs must be automatically processed, contextualized, and converted into an easily digestible format for the user.

-The service must allow for scalable search queries with a minimum of 250 queries per day.

-The service shall be 28 CFR Part 23 compliant.

Dashboard/user interface:

-The capability must have the functionality to view all threat intelligence feeds, open source information, social media sites, and publically available information in one location.

-Discovery and Filtering functionality of information by Indicators of Threats or Compromise; hash tagging search, trending, and analysis capability (discovery of malicious activity), keywords, last name, first name, rank, date, username monikers, DarkWeb market places, email addresses, physical addresses, and social media venue.

-Drill down functionality for individual incident or alert by entity name, profile URL/unique identifier, date, social media venue, imagery, internet protocol (I.P. address), I.P ports, and malicious links.

-Machine Learning algorithm to present a risk rating and/or confidence score of harvested threat intelligence.

Bulk reporting, visualization, and exportable features:

- The software and service shall have the capability to download and export the results of the query in a format that will allow for visualization/link analysis and bulk reporting (MS Word, Adobe PDF and .csv).

- There shall be visualization using direct graphs for link analysis with 1 to 1 correlations as well as multiple relationships to facilitate analysis of the data. This function shall also allow for the integration of our agency's internal data.

- The capability/solution must be able to deliver threat reporting outside of the SaaS (e.g. email addresses and SMS) that is tunable by the end user.

Data Retention and Storage:

- Vendor shall state whether or not they will be retaining the data at a U.S. based physical data center or on a cloud based bucket, or they are going to allow CID to do it. Customer requires data to be secured and maintained by vendor. Vendor will identify who will have access to this data (e.g. system engineers or system administrators).

-The service shall allow for the search of archived data gathered as a result of established queries/on-going collection efforts.

Service Level Agreement (SLA):
-24/7/365 Technical Helpdesk Support must be provided to Government users.

-System uptime of 99.97% and shall inform the designated representative(s) (e.g. the Contracting Officer's Representative, "COR") in writing no less than 2 weeks prior to any scheduled maintenance or planned outages that may degrade or interrupt service or user access to the system.

-The capability shall be accessible to the Government user 24hr/7days/365.

-The vendor shall notify the Government within 24 hours of losing access to any data source.

Additional Requirements:

- The service shall be capable of real-time persistent (via map overlays) geospatial and geo-location search analysis across multiple sources. This SaaS will allow the user to gather, display, and manipulate imagery, GPS, satellite photography and historical data, described explicitly in terms of geographic coordinates or implicitly, in terms of a street address, postal code, or forest stand identifier as they are applied to geographic models. This capability must allow analysts to read and analyze all message traffic (tweets, videos, images, etc.) in regard to that particular location. All message traffic feed shall have visualizers such as word clouds, pie charts, bar graphs, etc.

- The software shall be capable of facial recognition, object detection, and license plate detection.

- The software shall be capable of reverse image searching, facial and object matching, and alerting when an object is already queried or already in an existing or third party database.

- The software shall be capable of indexing and querying advertisement identification (AdTech) data.

- The service shall provide real-time data aggregation, organization and visualization with scoring of search results.

- The service shall provide direct access to collected media on target entities.

- The service needs to have persistent, real-time keyword monitoring, which allows the user to modify as required.

3.2 - Training

Vendor shall provide three training courses (One training course at each location of Quantico, VA; Hunter Army Air Field, GA; and Joint Base Lewis-McChord, WA) annually for up to 25 students per training session. This course shall be an interactive course and shall be uniquely designed as to introduce attendees on how to effectively utilize the SaaS Solution to research social media sources. Training dates shall be coordinated with the USACIDC within two (2) working days of contract award to select the best suitable dates to conduct training. The first training session shall be conducted no later than 30 days after contract award unless later date is identified by USACIDC.

The training locations are as follows:

HQ USACIDC
Russell-Knox Building
27130 Telegraph Rd
Quantico, VA 22134

Hunter Army Air Field, GA:
2182 South Perimeter Road
Hunter Army Airfield, GA 31409

Joint Base Lewis-McChord, WA
31310 Pendleton Ave
Joint Base Lewis-McChord, WA 98433

4.0 DELIVERY SCHEDULE:

The contractor shall provide necessary information or instructions on how to receive the 13 Subscription Services within two (2) working days after contract award. Training dates shall be coordinated with the USACIDC within two (2) working days of contract award to select the best suitable dates to conduct training. The first training session shall be conducted no later than 30 days after contract award.

5.0 CONTRACT TYPE:

Firm Fixed Price (FFP) type contract.

6.0 INSPECTION/ACCEPTANCE TERMS:

Inspection and acceptance shall be at destination.

Point of Contact (POC):
Name: Joseph Smith
Phone: (571) 305-4316
Email: joseph.a.smith.civ@mail.mil

7.0 DELIVERY LOCATION:

HQ USACIDC
Russell-Knox Building
27130 Telegraph Rd
Quantico, VA 22134

Point of Contact (POC):
Name: Joseph Smith
Phone: (571) 305-4316
Email: joseph.a.smith.civ@mail.mil

8.0 Anti-Terrorism (AT) Level I Training:

8.1 For contractor employees with an area of performance within Army controlled installation, facility, or area: Contractor and all associated sub-contractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity

Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

8.2 For contractors that do not require CAC, but require access to a DoD facility or installation: Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

9.0 RECOGNIZED HOLIDAYS:

New Year's Day
Martin Luther King Jr.'s Birthday
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day