PERFORMANCE WORK STATEMENT (PWS)
ENFORCEMENT AND REMOVAL OPERATIONS (ERO)
TARGETING OPERATIONS DIVISION (TOD)
FOR
LEAD DEVELOPMENT and
OPEN-SOURCE INTELLIGENCE / SOCIAL MEDIA CONTRACT

1.0 GENERAL

1.1 BACKGROUND

Removing aliens present in the United States (U.S.) who have violated U.S. laws is a national public safety priority. To address these threats, Immigration and Customs Enforcement (ICE) formed the Targeting Operations Division (TOD) within the ICE Enforcement and Removal Operations (ERO) directorate. The primary mission of the TOD is to identify and locate aliens that pose a threat to public safety or national security. The TOD has a current and recurring need for analytical services in support of its mission to identify and locate individuals who have violated U.S. laws. This support includes the analysis of information obtained from commercial and law enforcement databases as well as publicly accessible, open-source and social media platforms.

Successful law enforcement operations require adaptation to changing public safety threats and the ability to continually refine processes and modernize information technologies. Although ICE-ERO continues to make considerable progress in identifying, targeting, and arresting individuals who have violated U.S. laws, the continued use of proactive and modern enforcement tools remains an essential approach to achieve ICE enforcement goals. Analysis of information sources is needed to enhance ICE's mission and program efficiency. Previous approaches to targeting individuals for enforcement action which have not incorporated open web sources and social media information, have had limited success. The individuals targeted for enforcement action purposely employ countermeasures to inhibit ICE-EROs ability to locate them.

1.2 OBJECTIVE

The objective of this effort is to perform analysis of information sources to obtain real-time and mission critical person-specific information, which may include but is not limited to addresses, vehicles, associates, etc. This information is necessary to support the TOD comprised of the National Criminal Analysis and Targeting Center (NCATC) in Williston, VT and the Pacific Enforcement Response Center (PERC) in Santa Ana, CA on immigration enforcement cases aligned with agency priorities and goals.

1.3 SCOPE

The scope of this effort includes analytical and lead generation services in support of the TOD's mission to locate individuals who pose a danger to national security, public safety, and/or otherwise meet ICE's law enforcement mission. The contractor will research and analyze data from commercial and law enforcement databases as well as other publicly accessible, open-source, and social media platforms to support investigations and aid in targeting individuals for arrest in furtherance of ICE law enforcement missions. The contractor shall compile, analyze, organize, and transmit all information obtained to ICE personnel. Contractor staff will be located onsite at either the NCATC government facility in Williston, VT or the PERC government facility in Santa Ana, CA. NCATC and PERC staff shall have the ability to interface directly with onsite contractor personnel and have immediate access to the requested information. Offsite work situations may be considered on a case-by-case basis due to extenuating circumstances. The COR or senior management (i.e. Supervisory Detention and Deportation Officer with minimum grade of GS-14) may authorize short-term or long-term exceptions to the onsite work requirement.

This contract will require one (1) Program Manager managing both sites, sited at the National Criminal Analysis and Targeting Center, as well as additional site-specific contractor staffing as noted below.

Minimum Staffing requirements for the NCATC are:

Place of Performance	Labor Category	Full-Time Equivalents
NCATC	Program Manager	1
	Site/Lead Senior Analyst	1
	Analyst	10
Total	--	12

1. One (1) NCATC Senior Analyst/Site Lead (designated as Key Personnel) – the core hours of this position will be Monday through Friday, 7:00 am to 6:30 pm (Eastern Time), with ready availability after-hours and on weekends. Approximately 25% of the NCATC's Senior Analyst/Site Lead's workhours may occur after hours, on weekends or during holidays.
2. Analysts - Staffing must be sufficient to ensure a minimum of 10 analysts are always available during NCATC hours of operation. To cover after-hour requirements and emergency situations, the contractor will establish a duty rotation consisting of a primary analyst, a secondary backup analyst, and the ability to call upon at least three (3) analysts as needed to ensure coverage.
3. Optimal Analyst coverage at the NCATC shall be scheduled with the goal of minimizing work disruptions during shift changes. The vendor will have discretion on staffing shift changes, while ensuring minimum coverage is maintained.

Minimum Staffing requirements for the PERC are:

Place of Performance	Labor Category	Personnel Required
PERC	Site Lead	1
	Senior Analyst/Shift Lead	3
	Analyst	12
Total	--	16

1. One (1) PERC Senior Analyst/Site Lead (designated as Key Personnel) – the core hours of this position will be Monday through Friday, 7:30 am to 5:00 pm (Pacific Time), with ready availability after-hours and on weekends. Approximately 25% of the Program Manager/Site Lead's workhours may occur afterhours, on weekends and during holidays.
2. Senior Analyst/Shift Lead (designated as Key Personnel) – staffing must be sufficient to ensure a minimum of one (1) on-site Senior Analyst/Shift Lead at all times during PERC's 24 hours per day, 7 days per week, 365 days per year operational schedule.
3. Analysts - staffing must be sufficient to ensure a minimum of three analysts at all times during PERC's 24 hours per day, 7 days per week 365 days per year operational schedule.
4. Optimal Shift Lead and Analyst coverage at the PERC shall be scheduled with the goal of minimizing work disruptions during shift changes. The vendor will have discretion on staffing shift changes, while ensuring minimum coverage is maintained.

1.4 APPLICABLE DOCUMENTS

1.4.1 COMPLIANCE DOCUMENTS

The following documents provide specifications, standards, or guidelines that must be complied with to meet the requirements of this task order (the most recent version is applicable):

1) Department of Homeland Security (DHS) MD Number 140-01, Information Technology (IT) Systems Security, the DHS Sensitive Systems Policy Directive 4300A, and the accompanying handbook, DHS 4300A Sensitive Systems Handbook:

2) DHS MD Number 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information;

3) DHS MD Number 11056.1, Sensitive Security Information (SSI);

4) DHS Directive Number 121-01, Office of the Chief Security Officer, Instruction Handbook Number 121-01-007, The DHS Personnel Security, Suitability and Fitness Program, Instruction Handbook Number 121-01-011, Department of Homeland Security Administrative Security Program;

5) DHS Privacy Incident Handling Guidance;

6) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information:

7) DHS Instruction 121-01-007-01, Revision 01, The Department of Homeland Security Personnel Security, Suitability and Fitness Program: and

8) DHS Sensitive Systems Policy Directive.

Note: All DHS specific documentation cited above will be available to the contractor following award.

2.0 SPECIFIC TASKS

2.1 LEAD DEVELOPMENT and LEAD ENHANCEMENT

2.1.1 The contractor shall screen, prioritize, and develop leads on incoming cases; enter leads into the leads management system of record; identify key targeting data (e.g. addresses, vehicles, places of employment; associates, etc.); collect and include additional intelligence of value to officer and operational safety, pattern(s) of travel, and potential criminal activity/criminal indicators. Ensure data fields in the system of record, are updated, accurate, and complete. Attach pertinent photographs, reports, and correspondence. Once entered, leads will be reviewed by PERC or NCATC federal staff for accuracy, quality and completeness before disseminating them to ICE Field Offices.

2.1.2 The government may require lead enhancements in certain cases. A lead enhancement involves a more detailed investigation and analysis to develop targeting data deemed critical to ICE law enforcement efforts. Actions to enhance leads involve a deeper dive to identify a more holistic case analysis, including open-source and social media enhancement of urgent and priority cases to collect additional intelligence of value to officer and operational safety, pattern(s) of travel, associates and potential criminal activity/criminal indicators.

2.1.3 The contractor shall develop and/or enhance leads as directed by TOD staff or with the following priorities in mind:

- **URGENT**: National security threats (domestic or international terrorism); ICE/ERO Top 10 Most Wanted; high profile and/or time sensitive enforcement actions; convictions of egregious crimes (e.g. murder, rape, etc.); escapees.
- **HIGH**: convicted of aggravated felony; convicted of 3 or more felonies, regardless of severity; convicted of a violent felony; arrested for egregious crime; wanted for egregious crime (foreign fugitive, human rights violator); security threat group (SATG, TCO, etc.)
- **NORMAL**: convicted of a non-violent felony; convicted of a violent misdemeanor.
- **LOW**: convicted of a non-violent misdemeanor; no convictions but has a significant arrest history.
- **Note**: Given the rapid and dynamic nature of ICE operations, the contractor must be flexible shifting priorities.

2.1.4 The targeted timelines for ***lead development*** associated with these priorities is:

- URGENT = 30 minutes; HIGH = 1 hour; NORMAL = 3 hours; LOW = 8 hours.

2.1.5 The targeted timelines for ***initial lead enhancement*** associated with these priorities is:

- URGENT = 1 hour; HIGH = 2 hours; NORMAL = 4 hours; LOW = 8 hours.

2.1.6 The NCATC or PERC designee may actively coordinate the prioritization of cases based on agency requirements, mission objectives, and the nature of each case. The government designee will communicate these priorities directly to the contractor to ensure alignment with ICE's enforcement goals and operational needs.

2.1.7 Performance goals: minimum acceptable performance is 75% of cases completed within specified timeframes. Greater than 85% completion rates are considered Very Good; Greater than 95% completion rates are considered Exceptional.

***Note**: The day-to-day supervision and direct control over the work performed by Contractor personnel shall be the sole responsibility of the Contractor.*

2.2 COLLECTION AND ANALYSIS OF DATA SOURCES

2.2.1 The Contractor shall use a wide range of commercial and law enforcement databases as well as internet-based open-source, deep web, social media and darknet sources, to collect, analyze and evaluate criminal intelligence information; locate and provide person-specific location information; coordinate and prepare enhanced lead packages and other lead products for dissemination to field office personnel. These activities are specific to individuals who pose a danger to national security, risk public safety or otherwise meet ICE enforcement priorities. The Contractor shall also provide other information relevant to enforcement actions as required.

The Contractor will use a wide range of information sources including publicly available internet-based social media platforms such as Facebook, Google+, LinkedIn, Pinterest, Tumblr, Instagram, VK, Flickr, Myspace, X (formerly Twitter X), TikTok, Reddit, WhatsApp, YouTube, etc. This may include the collection of any public messages (e.g., "Tweets"), postings, and other media/data (e.g., photos, documents such as resumes, geocached information, etc.). The Contractor may also be provided access to available commercial databases (e.g. Thomson Reuters' CLEAR® and LexisNexis' Accurint®), government-owned databases (e.g. Person Centric Query Service (PCQS)), law enforcement specific query databases (e.g. ACRIME, ELITE, PCIS, PCQS, EARM, ADIS and ELIS) and other databases as required (what about PACER?). Commercial source search capabilities and databases subscribed to by the Contractor may also be used following approval from the COR.

2.2.2 A time and material line item is included to authorize reimbursement of up to $1,100,000 annually for subscription-based third-party databases, search tools, etc. that enhance the quality and timeliness of work required under this contract. This cost-reimbursement is not intended to offset the cost of vendor's ***current*** subscriptions, rather for the addition of ***new*** subscription tools. The vendor shall recommend tools for advance approval by the COR, outlining the benefits to the government.

2.2.3 The Contractor shall search and return data 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, Social Security Number (SSN) changes, utility changes, credit checks, death registry information, employment changes, insurance changes, affiliated organization, and other information as required by which a location can be derived. Tier one (1) level data is information directly connected to the target. Search results directly connected to the target that also contain information related to the target's associates shall be included with all Tier 1 information provided.
2.2.4 In addition to the above, the government may request that the contractor also search and return data that includes available information about the target's associates, such as family members, friends, or co-workers, through which the location of the target may be derived. These searches may be conducted using the sources described above.

2.2.5 The Contractor shall provide ERO personnel with timely, clearly written leads and reports of good quality that document search results. Investigations will vary in complexity with completion times generally ranging from four (4) hours up to several days. An analyst must have a referral rate of at least 35 percent of all cases assigned per month. Referrals also include cases where the target has left the U.S, is incarcerated, or is deceased. The Contractor must advise the COR in advance if the referral rates or productivity will be less than expected.

2.2.6 The Contractor shall develop an automatic assigning and tracking system for cases assigned, worked and pending, which must be easily accessible by government staff. Ownership of the tracking system, including all associated data and functionality, shall reside with the government; however, the tracking system will be developed and maintained by the contractor and will be jointly managed by federal staff and the contractor, with full access to both parties as necessary to fulfill their respective responsibilities.

2.2.7 The Contractor shall maintain knowledge of and apply a broad variety of instructional materials, guides, and manuals to support the development of new processes and methods for the collection and analysis of this intelligence information and generation of leads.

2.2.8 The contractor must provide monthly information sessions, delivering clear and concise overview of capabilities under this contract, to all ICE field offices, and HQ programs. The monthly information sessions will be scheduled as needed and are expected to last no more than an hour.

2.2.9 The Contractor shall meet with the Contracting Officer, COR and NCATC/PERC Technical SME(s) as necessary to discuss elements of the effort including but not limited to performance issues, emergency situations, etc. The Contractor shall respond to meeting requests regarding emergency situations within 30 minutes during normal duty hours and within two hours after normal duty hours. Written minutes for all meetings shall be prepared by the Contractor, signed by the Contractor's designated representative, and furnished to the Government within two (2) workdays of the subject meeting.

Except for queries conducted in government-owned law enforcement specific databases, or other systems approved by the COR, only data sources that are open to the general public (open source) in the U.S. and in foreign jurisdictions are permitted for use under this effort. R Contractor

personnel must adhere to the following requirements and DHS policies when performing tasks under this effort:

1) Obtaining Information from Unrestricted Sources. The Contractor may obtain information from publicly accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.
2) Accessing Restricted Sources. When conducting searches, the Contractor **may not** access restricted online sources or facilities.
3) Obtaining Identifying Information about Users or Networks. The Contractor **may not** use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.
4) Public Interaction. The Contractor may access publicly available information only by reviewing posted information and **may not** interact with the individuals who posted the information.
5) Appropriating Online Identity. "Appropriating online identity" occurs when an entity electronically communicates with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. The Contractor **may not** use this technique to access information about individuals.
6) PII Safeguards. The Contractor will protect personally identifiable information (PII) as required by the Privacy Act and DHS privacy policy.
7) Unless gathering information from online facilities is configured for public access, the Contractor should make reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located within a foreign jurisdiction. Whenever an item or person is located outside the United States or its territories, the Contractor must notify the Government.
8) The Contractor shall not maintain outside of the ICE computer network: 1.) any person-specific data, including lists of targets provided by the Government; 2.) search results provided to the Government after the analysis is complete. The Contractor shall not maintain person-specific data on behalf of the Government 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 the Government for any outside commercial purpose.

3.0 DELIVERABLES AND DELIVERY SCHEDULE

The following deliverables are to be provided electronically via e-mail no later than the due dates specified below to the contracting officer and COR. All deliverables shall conform to NCATC formatting requirements; proprietary formatted documentation is not acceptable unless approved by NCATC. All deliverables require review and acceptance by the COR. All documentation or databases (e.g., deliverables, software releases, source code, tracking database etc.) developed by the contractor shall become the sole property of the U.S. government.

Documentation shall not include brands, logos or other marks identifying ownership or authorship besides the government. In fulfillment of this effort, the contractor shall be responsible for maintaining and reporting accurate and current reports. All deliverables shall remain consistent with all applicable DHS guidance.

3.1 PROJECT MANAGEMENT PLAN

The contractor shall prepare and submit a project management plan. The initial draft of the Project Management Plan is due 10 business days after the award. The government will have five (5) business days to review and provide comment(s), and the contractor shall have five (5) business days to make changes and submit a final draft. The project plan, at minimum, shall address the following elements:

1) 60-day transition plan from the incumbent contractor that includes a description of the procedures used for measuring and reporting transition progress (including Work Breakdown Structure).
2) Critical milestone schedule (e.g., staffing, logistics).
3) Applicable deliverables.
4) Planning, monitoring and control system including a description of the techniques used to identify, monitor and control technical and program risks; and
5) Other project information if required.

3.1.1. CONTINGENCY PLAN

The contractor shall prepare, submit and maintain a detailed Contingency Plan (CP) as part of its project management plan. The CP shall describe the contractor's ability to expand operations and/or work at an alternate work site during special contingency situations including but not limited to structural fire, accidents, civil disturbances, disaster warnings, acts of God, public health emergencies, national emergencies and international crisis. The contractor shall be required to update this contingency plan annually following task order award.

3.1.2. QUALITY CONTROL PLAN

The contractor shall prepare, submit and maintain a detailed Quality Control Plan (QCP) as part of its project management plan. All work to be accomplished under this PWS shall be managed by the QCP. The contractor is solely responsible for the quality of services provided and is also liable for contractor employee negligence, and any fraud, waste or abuse. The contractor's QCP shall ensure services and deliverables are completed in accordance with applicable government

regulations and instructions, and meet specified acceptable levels of quality, subject to government approval. To accommodate changing priorities and work requirements, the QCP may be revised as needed, but not more often than monthly, throughout the period of performance. Revisions shall be approved by the COR. At a minimum, the contractor's QCP shall include the following:

1) Performance metrics to measure the quality of work and productivity levels of contractor personnel.

2) An internal quality control and inspection system for required services. The job titles and organizational positions of the individuals who shall conduct the inspections must be specified.

3) A method to identify deficiencies in services and deliverables.

4) Procedures to correct any deficiency in services or deliverables.

The contractor must maintain records regarding inspections and other quality and internal control actions that document the purpose of the inspection, the results of the inspection, and any corrective action taken as a result of the inspection. Upon request, these records shall be made available to the government during the period of performance.

3.2 MONTHLY/WEEKLY STATUS REPORTS

The contractor shall prepare and submit a monthly status report due on the 10th day of each month. Monthly progress reports, at minimum, shall detail progress made during the prior month, progress expected during the next month, resources expended, any significant problems or issues encountered, recommended actions to resolve identified problems and any variances from the proposed schedule.

The Contractor shall prepare and submit a weekly statistical report due every Monday for the previous week, Sunday to Saturday. Weekly Reports shall include number of cases referred to the Contractor; number of cases completed by the Contractor; and number of cases pending.

3.3 STANDARD OPERATING PROCEDURES

All work to be accomplished under this PWS shall be managed via formal Standard Operating Procedures (SOPs). The SOPs shall document how all services will be approached and accomplished. Initial SOPs are due 20 business days after the award. The government will have five (5) business days to review and provide comments, and the contractor shall have five (5) business days to make changes and submit a final draft. To accommodate changing priorities and work requirements, SOPs may be revised as needed, but not more often than monthly, throughout the period of performance. Revisions shall be approved by the COR.

4.0 CONTRACTOR PERSONNEL

4.1 QUALIFIED PERSONNEL

The contractor shall provide qualified personnel to perform all requirements specified in this PWS, and ensure they are physically present at the NCATC and PERC. Contractor personnel must also be cross trained to support both TOD centers as needed. The contractor is expected to have COR approved employees in place and on duty at the NCATC and PERC within 30 business days after award, with emphasis on permanent staff. Ongoing rotations of temporary contractor personnel will not be allowed.

4.2 CONTINUITY OF SUPPORT

The contractor shall ensure that the contractual required level of support for this requirement is always maintained. The contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the contractor shall provide e-mail notification to the COR prior to employee absence. Otherwise, the contractor shall provide a fully qualified replacement.

4.3 KEY PERSONNEL

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer's Representative no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. The Program Manager/Site and the shift leads are designated as Key for this requirement.

4.3.1 PROGRAM MANAGER

The Program Manager (PM) will be onsite and physically present at the NCATC and keep regular business hours as determined by the NCATC operations. The program manager will also supervise contractor personnel and manage all workload and schedules while serving as the primary liaison between the contractor and the government. The program manager shall provide adequate guidance and oversight to other contractor personnel to ensure the quality and timeliness of work meets or exceeds government requirements. The program manager will ensure that all contractor personnel adhere to all government policies, procedures, and guidelines. The Program Manager will also provide statistical information to the contractor and to the government as needed. The program manager will also share knowledge and expertise about research techniques with government employees, both formally in a training setting or informally during casework. The program manager will ensure that cases are assigned according to the designated priority and will inform the COR when additional casework is needed or when the caseload requires additional support from all contractor personnel.

The Program mManager should have the following experience/qualifications: 1) At least 10

years of cumulative experience in performing investigations to include but not limited to social media and open source information, research, targeting and analysis; 2) Sound knowledge of immigration and criminal justice laws, regulations, and policies; and 3) At least two years of supervisory or team leader experience and experience managing a team workload with competing priorities and deadlines.

Note: This Program Manager shall be responsible for the management and performance of all work under this task order. The Government will have the right to approve the PM selected for this effort. The PM shall be the primary point of contact for the Contracting Officer and designated COR.

4.3.2 SENIOR ANALYST/SITE LEAD

The Senior Analysts/Site Leads will assist the Program Manager with supervising contractor personnel at each site and manage all site-specific workload while serving as an additional designated liaison between the contractor and government. Senior Analysts/Site Lads shall provide adequate guidance and oversight to other contractor personnel to ensure the quality of work meets or exceeds government requirements. Senior Analysts will ensure that all contractor personnel adhere to all government policies, procedures, and guidelines. Senior Analysts will also provide statistical information to the contractor and to the government as needed. All administrative functions performed by Senior Analysts shall not exceed more than 10 percent of any workday without permission from the COR. Senior Analysts will also share knowledge and expertise about research techniques with government employees, both formally in a training setting or informally during casework. Senior Analysts will ensure that cases are assigned according to their priority and will inform the COR when more casework is needed or when the caseload requires support from all contractor personnel on the contract regardless of office location.

Senior analysts/Site Leads should have the following experience/qualifications:

1) At least five (5) years of cumulative experience in performing investigations to include but not limited to social media and open-source information, research, targeting and analysis;

2) 2) Advanced knowledge of immigration and criminal justice laws, regulations, and policies; and
3) 3) Ability to supervise and lead a team and manage a team workload with competing priorities and deadlines.

Note: The contractor shall designate the Senior Analyst/Site Lead as the overall Task Order Program Manager (PM) specific to each site (NCATC or PERC) in the PM's absence. This Senior Analyst/Site Lead shall be responsible for the management and performance of all work under this task order at their respective site (NCATC or PERC). The government will reserve the right to approve the Senior Analysts/Site Leads selected for this effort. The Senior Analyst/Site Lead shall be the primary point of contact for the contracting officer and designated COR in the PM's absence.

4.3.4 ANALYST

Analysts will perform research and analysis of myriad data sources and initiate leads in accordance with this PWS.

Analysts should have the minimum following experience/qualifications:

1) Bachelor's degree or higher and one (1) years' experience performing primarily social media and open-source information research, targeting, and analysis; or,

2) Associate's degree and two (2) years' experience performing primarily social media and open-source information research, targeting, and analysis; or,

3) High school diploma or GED three (3) years' experience performing primarily social media and open-source information research, targeting, and analysis.

4)

4.4 REQUIRED DUTY HOURS

The contractor shall provide support in accordance with NCATC Duty hours (i.e. Monday through Friday 7:00 am to 6:30 pm (Eastern Time) or PERC Duty hours (24x7, 365 days per year). The contractor's work hours are to be aligned with the NCATC's and PERC's established hours. Additionally, given the nature of the ICE law enforcement mission, this work contract is deemed mission essential and work will be expected to continue during government shut downs. Telework and remote work is not generally authorized. However, in extenuating circumstances telework and remote work may be authorized on a case-by-case basis with written Telework authorization by the COR in accordance with agency policies.

For the PERC, telework and remote work are authorized for contractor personnel supporting the PERC location in California to facilitate contract performance. However, if performance falls below a "Good" rating, telework and remote work may be adjusted or revoked on a case-by-case basis, subject to written approval by the COR and in accordance with agency policies.

4.5 GOVERNMENT HOLIDAYS

The following government holidays are normally observed by government personnel: New Year's Day, Martin Luther King's Birthday, Presidential Inauguration Day (metropolitan DC area only), President's Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, Christmas Day, and any other day designated by Federal Statute, Executive Order and/or Presidential Proclamation. Given PERC's 24x7, 365 days per year operational schedule, coverage at the PERC must be maintained during all Government holidays.

4.6 ON-CALL EMERGENCY SUPPORT

The contractor shall provide on-call emergency support 24 hours a day, seven (7) days a week, including holidays, in response to high-priority ICE operational taskings or any other emergency. The contractor shall provide weekly information to the COR with the names and

phone numbers of the primary and alternate points of contact, as well as a POC responsible for oversight of any issues, in particular issues regarding contacting the assigned duty analysts. The contractor shall respond to any inquiry or problem within one hour of initial contact.

4.7 TRAINING

The contractor shall ensure prior to and throughout their employment under this PWS, that all contractor personnel possess appropriate Industry Standard training, skills, experience, certificates and/or degrees required to adequately perform all tasks related to their labor category at no cost to the government. However, the government will provide contractor personnel with appropriate training to ensure that they have a working understanding of NCATC operations, immigration law, data systems, and procedures, as well as rules on the operational use of social media. The contractor shall complete all government-provided training required to maintain access to the DHS network. If additional training by the government is needed to ensure efficient operation of the contract, the contractor will make a formal request to the COR for review and approval.

5.0 OTHER APPLICABLE CONDITIONS

5.1 GOVERNMENT QUALITY ASSURANCE

The government shall monitor the contractor's performance using a Quality Assurance Surveillance Plan which incorporates the following elements:

1) Timeliness – Turn-around-times based on priorities.

2) Standards – Review of reports and contractor records and logs.

3) Quality Control Records – Reviews contractors quality control records and quality system records as applicable to determine if contractor’s plan is being followed.

4) Customer Service—ad-hoc feedback from employees about contractor’s product and professionalism.

5) Productivity measures – (value and outcome of product contribution to the enforcement mission).

Goal 1: Timely, Accurate Production

- Specific: Complete social media analysis requests and produce reports that meet established deadlines.
- Measurable: Achieve 95% on-time completion with an error/rework rate below 5% (per supervisor review).
- Achievable: Analyst has access to necessary open-source intelligence (OSINT) tools and training to meet deadlines.

- Relevant: Supports mission by ensuring decision-makers have timely, credible information.
- Time-bound: Measured quarterly.

Goal 2: Mission Impact

- Specific: Provide actionable OSINT products that support enforcement, investigative, or partner-agency objectives.
- Measurable: Ensure at least 2 analytic products per quarter are directly cited in operational actions, case files, or partner reports.
- Achievable: Analyst will prioritize requests tied to active operations and emerging threats.
- Relevant: Directly connects analyst's work to mission-critical outcomes.

Goal 3: Collaboration & Knowledge Sharing

- Specific: Engage in interagency collaboration and contribute to workforce development.
- Achievable: Analyst will collaborate with internal stakeholders to align on cases or OSINT trends.
- Relevant: Enhances partnerships and ensure broader agency adoption of OSINT best practices.
- Time-bound: Evaluated quarterly (initiatives).

5.2 GOVERNMENT-FURNISHED EQUIPMENT (GFE) AND INFORMATION

The government will supply the necessary working space, supplies, computer equipment, system access, and telephone equipment to work in a government facility. The government will provide access to all DHS systems and information needed by the contractors to perform their duties.

GFE will be managed in accordance with all applicable regulations.

5.3. PERIOD OF PERFORMANCE

The period of performance for this task order will include a one-year base period with four (4), one-year option periods and is anticipated as follows:

Transition-In	May 7, 2026, through Jul 6, 2026
Base Period	July 7, 2026, through May 6, 2027
Option Period One	May 7, 2027, through May 6, 2028
Option Period Two	May 7, 2028, through May 6, 2029
Option Period Three	May 7, 2029, through May 6, 2030
Option Period Four	May 7, 2030, through May 6, 2031

5.4 PLACE OF PERFORMANCE

The primary places of performance will be onsite at the following government facilities:

National Criminal Analysis and Targeting Center (NCATC)
426 Industrial Avenue, Suite 170
Williston, VT 05495

Pacific Enforcement Response Center (PERC)
3 Hutton Centre Drive
Santa Ana, CA 92707

5.5 POST AWARD CONFERENCE

The contractor shall attend a post award conference with the contracting officer and the COR no later than **5** business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the contracting officer, is to discuss technical and contracting objectives of this task order. The post award conference will be held via teleconference. Further details regarding the post award conference will be provided following award.

5.6 SECURITY REQUIREMENTS

5.6.1 GENERAL

ICE has determined that the performance of the tasks described in the contract/task order no. TBD requires that the contractor, subcontractor(s), vendor(s), etc. have access to sensitive DHS information, and that the contractor will adhere to the following.

5.6.2 PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding or terminating unescorted at government facility and/or sensitive government information access for contractor employees, based upon the results of a fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary fitness determination based on preliminary security checks. The preliminary fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a full field background investigation. The granting of a favorable preliminary fitness shall not be considered as assurance that a favorable final fitness determination will follow as a result thereof. The granting of preliminary fitness or final fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the contractor shall be allowed unescorted access to a government facility without a favorable preliminary Fitness determination or final Fitness determination by OPR-PSU. Contract employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or

successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the fitness screening process. (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003).

5.6.3 BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporary employees, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the PSU. Contractor employees nominated by a contracting officer representative for consideration to support this contract shall submit the following security vetting documentation to OPR-PSU, through the COR, within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1) Standard Form 85P (Standard Form 85PS (with supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by the contractor employee in their OPM e-QIP account.

2) Signature Release Forms,three (3) total, generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by the contractor employee in their OPM e-QIP account.

3) Two (2) SF 87 (Rev. December 2017) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU).**

4) Foreign National Relatives or Associates Statement. (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account).

5) DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account).

6) Optional Form 306 Declaration for Federal Employment (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account).

7) If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) (This document sent as an

attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account).

8) One additional document may be applicable if a contractor employee was born abroad. If applicable, additional forms and instructions will be provided to contractor employee. (If applicable, the document will be sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account).

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under reciprocity. The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and the applicant has not had a break in service for more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01). Required information for submission of the security packet will be provided by OPR-PSU at the time of the award of the contract. Only complete packages will be accepted by the OPR-PSU as notified by the COR.

To ensure adequate background investigative coverage, contractor employees must currently reside in the United States or its Territories. Additionally, contractor employees are required to have resided within the Unites States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. Citizens are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007-001.

5.6.4 TRANSFERS FROM OTHER DHS CONTRACTS

Contractor employees may be eligible for transfer from other DHS Component contracts provided they have an adequate and current investigation meeting the new assignment requirement. If the contractor employee does not meet the new assignment requirement a DHS 11000-25 with ICE supplemental page will be submitted to OPR-PSU to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change." The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

5.6.5 CONTINUED ELIGIBILITY

ICE reserves the right and prerogative to deny and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in DHS Instruction 121-01-007-01, Chapter 3, paragraph 6.B or who violates standards of conduct under 6 CFR § 115.117. The contracting officer or their representative can determine if a risk of compromising sensitive government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support. The OPR-PSU will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued fitness of contractor employees.

5.6.6 REQUIRED REPORTS

The contractor will notify OPR-PSU, via the COR, of all terminations/resignations of contractor employees under the contract within five days of occurrence. The contractor will return any expired ICE issued identification cards and building passes of terminated/ resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the ID Unit responsible.

The contractor will report any adverse information coming to their attention concerning contracting employees under the contract to the OPR-PSU, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the contractor employees' name and social security number, along with the adverse information being reported.

The contractor will provide, through the COR a Quarterly Report containing the names of contractor employees who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation). The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

CORs will submit reports to psu-industrial-security@ice.dhs.gov

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information NDA for contractor access to sensitive information. The NDA will be administered by the COR to all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for the purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as performance work statements; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, DHS Policy for Sensitive Information and ICE Policy 4003, Safeguarding Law Enforcement Sensitive Information.

Any unauthorized disclosure of information should be reported to ICE.ADSEC@ICE.dhs.gov.

5.6.7 SECURITY MANAGEMENT

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all government information and data accessed by the contractor.

The COR and the OPR-PSU shall have the right to inspect the procedures, methods, and facilities utilized by the contractor in complying with the security requirements under this contract. Should the COR determine that the contractor is not complying with the security requirements of this contract, the contractor will be informed in writing by the contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

5.6.8 INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on department telecommunications and automated information systems, the contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1, Information Technology Systems Security, or its replacement. Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

5.6.9 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on the designated ICE training system or by contacting ICE.ADSEC@ICE.dhs.gov. Department contractor employees, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access department information systems will be continually evaluated while performing these duties. System administrators should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).