Attachment 1 - Skip Tracing Services Statement of Work Amendment 2

1.0 Background

The Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Office of Enforcement and Removals (ERO) has an immediate need for Skip Tracing Services. The total docket size is approximately 1.5M. Government furnished case data will be utilized with identifiable information, commercial data verification, and physical observation services, as described further below, to verify alien address information, investigate alternative alien address information, and confirm the new location of aliens to ERO.

2.0 Scope

The effort should include enhanced location research, which entails automated and manual real-time skip tracing, extensive research on Google and/or other search engines or applications, as determined in the vendor's discretion; and the collection of photos and documents verifying the alien's residence and/or place of employment. The vendor should prioritize the alien's residence but failing that will attempt to verify place of employment.

3.0 Definitions

"Attempted" means that the vendor visually observed and/or physically visited a location that, based on available information (including available information following enhanced location research), the vendor believed to be the location of residence or employment of the alien, and: (1) located the individual if required; (2) confirmed that the location was the location of residence or employment of the Alien; (3) confirmed that the location was not the previously provided residence/workplace of the alien; or (4) determined that the physical visit to the location provided inconclusive information as to the whereabouts of the alien.

"Visit" means an attempted physical, in-person surveillance and verification effort to validate that a location is the actual residence or employment address of the alien.

4.0 Required Services

It is anticipated that multiple vendors will be given a monthly caseload of approximately 50k last known addresses of aliens residing within the United States of America. As the vendor completes adjudication, additional case files may be provided. Caseload volume and frequency is

subject to adjustment. Prior to any physical, in-person surveillance and verification, the vendor should use all technology systems available to identify and validate the most recent addresses of the individuals provided by the Government. Technology can be COTS products, and the Government will accept the recommendations of the vendor. Multiple verification sources are recommended to achieve a high confidence level.

To achieve a higher level of confidence, the vendor may physically verify the alien's location and presence, preferably confirming their home or work location. The vendor will then report the physical location to the Government or inform the Government that it is not able to locate the alien, and any additional visits would be fruitless. The vendor should prioritize locating the home address and only resort to employment location, failing that.

The vendor will document each visit by providing a written description of the visit (including the amount of time spent travelling to and from the location and the amount of time spent at the location, and the outcome of the visit) and by providing time-stamped photographs of the location or an explanation of why obtaining photographic evidence was not appropriate in the circumstances.

During attempts to locate an alien, the vendor will not discuss the nature of the case with any other party.

The vendor must have a working knowledge / background in using investigatory tools to conduct advanced skip tracing using last known addresses.

5.0 Deliverables

The vendor, upon receiving and reviewing the information provided by the Government, will be required to provide recurring updates (daily or as specified by the Government) on the status of each file. These updates must include any newly identified information relevant to the case, ensuring accuracy and reliability.

Any updated information returned by the vendor must be of high confidence, supported by verifiable evidence, and the vendor must be able to document and justify their conclusions. Supporting documentation should be comprehensive and may include, but is not limited to:

- Photographs verifying a residential address.
- Copies of official documents, such as death certificates or court records.
- Utility bills or other proof of residency.
- Employment verification records.
- Any other relevant and credible documentation that substantiates the findings.

The vendor must also ensure compliance with all applicable laws and regulations governing data collection, privacy, and reporting. Additionally, the vendor should outline their methodology for skip tracking, including the tools and resources utilized, to ensure transparency and confidence in their processes.

The Government expects the vendor to maintain open communication and provide timely responses to inquiries or requests for clarification regarding any file. A detailed reporting structure and escalation process should also be included in the proposal to address any discrepancies or challenges encountered during the skip tracking process.

Vendors are encouraged to provide a clear timeline for implementation, a description of their experience and qualifications in skip tracking services, and any additional capabilities that may enhance the effectiveness of the service.

6.0 Security Requirements

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

Position Designation

IAW Title 5, CFR part 731, dated December 18, 2024, and 5 CFR 1400. Agencies are required to designate position risk and sensitivity level for all contractor employees to determine the commensurate level of background investigation. The public trust risk of a position is the assessment of the degree of potential damage to the efficiency or integrity of the service that could arise from misconduct by the incumbent in the position.

Therefore, once the contract is awarded and before the vendor starts submitting personnel for security vetting, the contractor will provide, through the Contracting Officer’s Representatives (CORs) a list of all positions, to include titles and specific description of the duties for each of positions assigned to support the contract.

Preliminary Fitness Designation

ICE will exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for contractor applicants/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 by the Office of Professional Responsibility (OPR), ICE Personnel Security Division (PSD). No employee of the contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination by OPR PSD. Contract employees are processed under 5 CFR 731 dated December 18, 2024, and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or successors 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)).

Background Investigations

Contractor employees (to include applicants, temporary, 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 OPR PSD. Contractor applicant/employees are nominated by a Contracting Officer Representative (COR) for consideration to support this contract via submission of the DHS Form 11000-25 and ICE Supplement to the DHS Form 11000-25 to OPR PSD. This contract shall submit the following security vetting documentation to OPR PSD, through the COR, within 10 days of notification of initiation of an Electronic Application for Background Investigations (eAPP), or successor thereto, in the Office of Personnel Management (OPM) automated on-line system:

1. Standard Form 85P (Standard Form 85PS (with supplement to 85P required for those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" form completed online and archived by the contractor applicant/employee in their NBIS eAPP account.

2. Signature Release Forms (Three total) generated by NBIS eAPP upon completion of Questionnaire (e-signature recommended/acceptable). Completed online and archived by the contractor applicant/employee in their NBIS eAPP account.

3. Electronic fingerprints taken at an approved facility **OR** two (2) SF 87 Fingerprint Cards (current revision) sent to OPR PSD. Additional information regarding fingerprints will be sent to the contractor applicant/employee from OPR PSD.

4. Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

5. Social Security Administration 89 form (SSA-89): Authorization for the Social Security Administration (SSA) to Release Social Security Number (SSN) Verification. This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

6. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

7. One additional document may be applicable if the contractor applicant/employee was born abroad. If applicable, the document will be sent as an attachment in an e-mail to OPR PSD from the contractor applicant/employee.

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 transfer of trust. The questionnaire related to 6 CFR § 115.117 listed above in item 5 will be required for positions designated under PREA. OPR PSD will determine if personnel meet transfer of trust requirements at the initial stage of processing and prior to requesting a new security questionnaire.

With respect to break-in-service requirements for transfer of trust, OPM removed the 24-month break-in-service provision. This requirement is replaced with a new process, established in the Federal Personnel Vetting Investigative Standards issued by the Suitability, Credentialing, and Security Executive Agents, which expands this window of time up to sixty months using a tiered, risk-based approach of graduated levels of investigation.

IAW 5 CFR 731 and E.O. 13764, the fixed five-year periodic reinvestigation for public trust positions and national security positions will soon be eliminated and only once personnel are enrolled in a continuous vetting program. Therefore, PSD will continue the reinvestigation process until this process is completed.

Required information for submission of security packet will be provided by OPR PSD at the time of award of the contract. Only complete packages will be accepted by OPR PSD as notified by the COR.

To ensure adequate background investigative coverage, contractor applicants/employees must currently reside in the United States or its Territories. Additionally, contractor applicants/employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor applicant/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 and Legal Permanent Residents 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, Revision 2, dated August 10, 2024. 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, Revision 2, dated August 10, 2024.

Continued Eligibility

ICE will exercise full control over granting, denying and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in 5 CFR 731 and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or who violate 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 Federal Government is transitioning to Trusted Workforce (TW) 2.0. TW 2.0 is a whole-of-government background investigation reform effort overhauling the personnel vetting process by creating a government-wide system that allows transfer of trust across organizations. All contractor employees will be subjected to the transition and will be enrolled into a continuous vetting system. Enrollment will include multiple requirements from all personnel and potential changes to processes, procedures, and systems. This contract will comply with all requirements that facilitate the mandated transition to TW 2.0.

OPR PSD will evaluate concerns received via multiple sources under the continuous vetting process, to evaluate continued Fitness of contractor employees. If concerns cannot be mitigated, the contractor will be removed from the ICE contract upon notification from OPR PSD.

Required Reports

The contractor will notify OPR PSD, via the COR providing an ICE Form 50-005, Contractor Employee Separation Clearance Checklist, of all terminations/resignations of contractor employees under the contract within five days of occurrence to the ICEDepartureNotification@ice.dhs.gov group box. 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 responsible ID Unit.

IAW DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, the Contracting Officer's Representatives (CORs) notify the servicing personnel and industrial security offices when a contractor employee is no longer working for DHS on any contract and report any derogatory information concerning the individual immediately, in accordance with the contract requirements. Report this information to

PSD-CEP-REPORTING@ice.dhs.gov. 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 (on a Microsoft Excel Spreadsheet) containing the names of contractor employees who are actively serving on their contract. 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. This list is what ICE Industrial Security uses to reconcile the contract quarterly. CORs will submit reports to PSD-Industrial-Security@ice.dhs.gov no later than the 10th day of each January, April, July and October.

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 Non-Disclosure Agreement (NDA) for contractor employee 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 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 statements of work; 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.

Security Management

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OPR PSD 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 OPR 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 to effect compliance with such requirements.

Information Technology Security

When sensitive government information is processed on Department telecommunications and automated information systems, the contract company 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 their access to Department IT systems and facilities terminated, regardless 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).

Information Technology Security Training and Oversight

In accordance with Office of the Chief Information Officer (OCIO) 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, Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT 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 ICE Training System (ITS) or by contacting ICE.ADSEC@ice.dhs.gov. 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).

7.0 Other Terms

The vendor shall ensure that the provision of these services is done in accordance with all terms of this contract and all applicable federal, state, and local law, with high standards of conduct, and with the use of qualified individuals with suitable training, education, experience, and skills to perform the services.