Background:

The Homeland Security Investigations (HSI) National Security Investigations Division (NSID) Counterterrorism and Criminal Exploitation Unit (CTCEU) combats national security vulnerabilities and prevents terrorists and other criminals from exploiting the nation's immigration system. The pursuit of these violators provides significant support to the "disrupt and deter" counterterrorism strategy of the U.S. CTCEU accomplishes its mission by reviewing the immigration status of known and suspected terrorists, by combating criminal exploitations of the Student and Exchange Visitor Program (SEVP), and by leveraging HSI's expertise with partnering agencies in identifying national security threats. CTCEU is the only national program dedicated to the enforcement of nonimmigrant visa violations.

CTCEU focuses its efforts on identifying and prioritizing, for enforcement action, foreign nationals who overstayed their period of admission or otherwise violated the terms or conditions of their admission to the U.S. CTCEU receives nonimmigrant compliance information from various investigative databases and Department of Homeland Security (DHS) entry/exit registration systems. The information identifies nonimmigrants who have entered the U.S. through an established immigration entry process and may have failed to comply with immigration regulations. Using a comprehensive prioritization scheme, CTCEU identifies nonimmigrant overstays, conducts in-depth analyses, locates targets, and initiates field investigations by referring high priority information to HSI Special Agents nationwide. CTCEU reviews over 1,000,000 violator leads for derogatory information annually and sends approximately 8,400 cases to HSI field offices for investigation.

DESCRIPTION OF REQUIREMENTS

The objective of this task order is to collect, research, analyze, and populate data in various law enforcement databases, as well as work with other government agencies at off-site locations. The Contractor shall be expected to meet operational demands and ensure timely responses to projects, daily requirements such as lead development and completion of weekly lead imports to ensure no backlogs develop, support operational components and timely submissions of deliverables.

The Government anticipates requiring continuation of the following tasks:

Task 1: Vetting and Screening.
The Contractor shall conduct searches of designated ICE systems, other government agency computer systems, and open source sites in order to identify violations and lead viability. The Contractor shall ensure that Contractor employees have or develop knowledge in the following:

- Terrorist organizations, history, operations, and tactics to include an understanding of how the various terrorist organizations operate.
- Illicit cross-border movement of people, cargo, vehicles, drugs, etc. and/or trade industry, to include identifying suspect trends and patterns.
- International criminal organizations (or international smuggling) and how the organizations operate and their areas of operation.

The Contractor shall perform analytical research and data analysis that includes, but is not limited to:

- Performing assessments on individuals, groups, financial institutions, commodities, and travel patterns on targets of interest.
- Having the ability to ingest and screen large volumes of Visa electronic applications efficiently and at high speed in regard DHS holdings in development of pre-adjudication information, derogatory and threat information assessment, adjudication recommendation to the Department of State and notification to other government equites when warranted.
- Providing case identification and tracking of IV and NIV applications at post through the application and adjudication process and provide electronic mechanism to push information to relevant partner programs systems and subsystems.
- Provide mechanism for scraping Visa issuance information to records and provide electronic mechanism to push information to relevant partner programs systems and subsystems.
- Provide multiple Metric solution capabilities in regard visa applicant, applications, VSPTS cases, ICM cases and trend analyses functions; provide external mechanism to validate the same information remotely. Provide electronic mechanism to push information to relevant partner programs systems and subsystems.

Task 2: Lead Generation.

The Contractor shall establish a team of highly trained analysts to perform case initiations, case reroutes, and case closures. These analysts shall be responsible for ensuring that each lead to the field is accurate and thorough. Additionally, these analysts shall provide investigative support to the field as needed. The Contractor shall generate a minimum of 10,000 investigative leads annually to the appropriate HSI field offices. To accomplish this, the Contractor shall provide:

- Automated lead review to determine lead viability.
- Process leads timely to ensure no backlogs occur on a monthly basis.
- Append viable leads daily to the case management database for further processing.
- Close non-viable leads daily in the LeadTrac Mod database management system.
- Develop strategies to exploit the various internal and external data sources to refine the intelligence analysis process.
- Implement process improvements and reengineer methodologies for modernization of systems and projects.
- Conduct bulk data extractions and insertions as required in LeadTrac Mod and Mongodb environment or other systems.

Task 3: Social Media Exploitation.

The Contractor shall leverage open source/social media to expand upon CTCEU's established abilities to utilize government and law enforcement databases in the investigation of national security and public safety concerns that exploit vulnerabilities in the U.S. immigration system by applying social media analytic capabilities, *derived only from free and publicly available sources through unattributed computers*, in numerous ways, including:

3.1 The Contractor shall use the open source information to identify actionable intelligence in addition to enhancing investigative findings, which includes, but is not limited to:

- Identification of recent valid addresses

- Investigation of cold cases
- Enhancement of subject identification
- Performing trend analysis
- Identification of criminal activity and derogatory information
- Identification of terrorist links and recruitment efforts displayed online

The Contractor shall analyze and apply techniques to exploit publically available information, such as media, blogs, public hearings, conferences, academic websites, social media websites such as Twitter, Facebook, and LinkedIn, radio, television, press, geospatial sources, internet sites, and specialized publications with intent to extract pertinent information regarding targets, including criminals, fugitives, nonimmigrant violators, and targeted national security threats and their location.

3.2 The National Security Investigations Division (NSID) seeks to develop a system to encompass the entire lifecycle of visa applicants from application through visa issuance, entry, departure, overstay or otherwise violation of the terms of admission into the United States.

Through the Visa Overstay Lifecycle pilot program, launched in August 2016, NSID visa screening operations are currently bifurcated and supported by two systems: the Visa Security Program's (VSP) Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT), and CTCEU's overstay enforcement system. PATRIOT identifies national security, public safety, and other visa eligibility concerns at the earliest point of an individual's visa application lifecycle. Upon entry to the United States, CTCEU then tracks the visa for the remaining validity and lifecycle.

The pilot project is designed to track the online activity of nonimmigrant visa holders that were issued in particular countries of concern from the time of application, through visa issuance, and entry into the United States. The project will conduct initial screening for social media presence and ongoing monitoring of social media activity, to continue during travel in the United States, until subsequent departure. This ongoing monitoring is focused on certain key indicators of emergent concerns, such as threats to public safety or affiliation with known or suspected terrorists or terror groups. Any derogatory information developed is then evaluated and referred for investigation and other actions as appropriate. In the event that the individual violates the terms and conditions of their admission to the United States or overstays their period of admission, the system allows HSI to leverage social media activity to locate and detain the individual. To enhance the Visa Overstay Lifecycle pilot program, the Contractor shall:

- Have the ability to ingest and screen against large volumes of visa electronic applications efficiently and at high speed in regard worldwide social media and open source holdings and domains relevant to person centric derogatory and threat information assessment information, adjudication recommendation to the Department of State and notification to other government equites when warranted. And, provide electronic mechanism to push information to relevant partner programs systems and subsystems.
- Develop a robust, overarching vetting process that would streamline the process to encompass the entire lifecycle of visa applicants from application through visa issuance, entry, departure, overstay, or otherwise violation of their terms of admission.

- Identify ways to more fully leverage social media as a tool to identify the whereabouts and activity of status violators, and provide enhanced knowledge about a nonimmigrant visitors' social media postings, from the adjudication of the visa application, through admission to the United States, and during their time in the United States.
- Take action to bridge the gap between what is done by VSP screening on the front end and what CTCEU systems do on the back-end.

Task 4: Government and/or Contractor Provided Training.
The Contractor shall provide a dedicated training team that will be responsible for all initial system and database training. The Government, on occasion, shall provide subsequent training, but not specific to lead generation. The Government will also provide occasional advanced training to contract staff. This may include, but is not limited to:

- FALCON
- Student and Exchange Visitor Information System (SEVIS)
- United States Visitor Immigrant Status Indicator Technology Registration System (US-VISIT)
- Central Index System (CIS)
- Computer Linked Automated Information Management System (CLAIMS)
- Refugee, Asylum & Parole System (RAPS)
- Consular Consolidated Database (CCDI)
- ENFORCE Alien Removal Module (EARM)
- Treasury Enforcement Communications System (TECS II)
- National Crime Information Center (NCIC)
- Consolidated Lead Evaluation and Reporting System (CLEAR)
- Automatic Targeting System – Passenger (ATS-P)
- Enterprise Document Management System (EDMS)
- Interim Case Management Solution (ICMS)
- Open Source Analysis (OS)
- Standard Operating Procedures for LeadTrac Mod and supporting systems, protocols, and tasks.

Task 5: Statistical / Data Review Support.
The Contractor shall provide statistical and data review support that includes, but is not limited to, the following:

- Analyze data integrity and consistency to obtain a quantitative basis for decision making and resource allocation.
- Provide intelligence and threat analysis of the information that is tailored to the government's requirements.
- Provide written reports and populate DHS databases or any other designated database as required.
- Provide specialized analysis related to data integrity, content of information, and production support in the Mongodb environment.
- Evaluate new technological capabilities to enhance productivity and efficiency.
- Conduct trend analyses and advanced technical research techniques to develop products based on the government's requirements.

- Extract data and develop reports from the LeadTrac Mod system as required.
- Create whitepapers and update Standard Operating Procedures as required.

Task 6: Ad Hoc Reporting.
The Contractor shall develop and produce qualitative intelligence reports, referred to as CTCEU reports, utilizing government databases and open source analysis for a comprehensive product. The Contractor shall provide an assessment package of the targets of interests to include; briefings, presentations, discussion panel participation, supporting documents and reports. The Contractor shall conduct research, generate reports, and assist with classified projects, as requested.