IMMIGRATION & CUSTOMS ENFORCEMENT
STATEMENT OF OBJECTIVES (SOO)
HSI DATA AND ANALYTICAL SERVICES

EXECUTIVE SUMMARY

U.S. Immigration and Customs Enforcement (ICE) protects America by dismantling transnational criminal organizations and enforcing immigration laws to preserve national security and public safety. ICE has offices in all 50 states and U.S. territories.

ICE has five main subcomponents: Homeland Security Investigation (HSI), the largest criminal investigative agency within the Department of Homeland Security (DHS) and the second largest investigative agency in the federal government; Enforcement and Removal Operations (ERO), which identifies, apprehends, and administratively removes illegal aliens from within the United States; the Office of the Principal Legal Advisor (OPLA) which serves as the exclusive representative of DHS in removal proceedings before the Executive Office for Immigration Review, litigating cases involving criminal aliens, terrorists, human rights abusers, and other aliens posing a threat to our homeland security; the Office of Professional Responsibility (OPR) which upholds ICE's professional standards through a multi-disciplinary approach of security, inspections, and investigations, and Management and Administration (M&A), which supports ICE by providing sound agency management.

HSI conducts criminal investigations against terrorists and other criminal organizations who threaten national security. HSI combats worldwide criminal enterprises who seek to exploit America's legitimate trade, travel and financial systems and enforces America's customs and immigration laws at and beyond the nation's borders.

This document provides the requirements and objectives needed to support ICE offices with contract support for aggregated data to include proprietary data and analytical services.

The intent of this requirement is to establish an Blanket Purchase Agreement (BPA) contract where any ICE entity may place individual calls. Each individual call is to be issued and managed through the organization desiring such services. HSI/Office of Intelligence (Intel) will identify the basic requirements, and any ICE organization may place calls against it. Each organization must assign its own Contracting Officer's Representative (COR), Alternate COR (ACOR), and Project Manager for their call and will be responsible for receiving, accepting, and processing their invoices for the services received. (In accordance with FAR 52.216-18)

The number of services identified herein are estimates only and are not purchased by this contract. The government may issue calls requiring performance at multiple locations, including any U.S. state or territory.

PURPOSE

The purpose of this procurement is to allow ICE organizations to quickly and efficiently engage the growing use of aggregated data to include proprietary data to precisely target criminal investigations of criminal, fraud, risk, and terrorism activity by utilizing data analysis to transform data into actionable insights. Obtaining these mission-critical analytic services will enable ICE to conduct customized analysis, screening, and monitoring of crime and fraud information. A data contract combined with professional analytical services provides ICE with access to information and the specialized expertise needed to process, analyze, visualize, and present that data in support of criminal investigations.

To be successful, law enforcement operations must adapt to changing public safety threats; thus, the ability to continually refine processes and modernize information technologies is mission critical. Agents and analysts must quickly and efficiently engage the growing use of data and data analysis technology to thwart criminal, fraud, risk, and threat activity. This includes more precisely targeting investigations by using data analysis to transform data into actionable insights. Data and analytical services are essential for conducting customized analysis, screening and vetting individuals and entities, developing lead information, and monitoring criminal and suspicious activities related to violations of the immigration and customs laws of the United States. The use of aggregated data, including propriety data, remains an essential approach to achieving agency goals. This contract requirement will support national security initiatives, maintain organization efficiencies, and allow leaders to focus resources on priority threats to public safety and/or national security.

Threats to homeland security include terrorist, transnational, and other criminal organizations that seek to exploit the customs and immigration laws of the United States. Accordingly, agents and analysts require immediate enhanced ability to identify, analyze, prioritize, disrupt, and dismantle transnational criminal organizations involved in the following:

- Narcotics and weapons smuggling/trafficking
- Transnational gang activity
- Financial crimes, money laundering and bulk cash smuggling
- Terrorism and terrorist activities
- Commercial fraud and intellectual property theft
- Cybercrimes including child exploitation and other Internet-enabled crime
- Human smuggling and trafficking
- Immigration, document and benefit fraud
- Human rights violations
- Intellectual property rights violations
- Export crimes
- International art and antiquity theft

An example of a specific mission related requirement is the combating of illicit fentanyl. Shared drug-related intelligence and trends are needed to address the threat from the shipments of illicit fentanyl, their precursors, and other synthetic drugs to the United States and elsewhere. These synthetics are then shipped and sold online from anonymous darknet markets and even overtly operated websites. It is extremely difficult for DHS, U.S. Customs and Border Protection (CBP),

HSI, and the U.S. Postal Inspection Service (USPIS) to address the threat due to the combination of the questionable legal status of these substances, the enormous volume of international parcel traffic by mail and express consignment couriers, and the technological and logistical challenges of detection and inspection. It is important to have access to global data combined with analytical expertise and services that can yield effective results for available real-time business, patent, scientific, shipping, finance, cyber and other data and information.

SCOPE

The scope of this requirement is to obtain use of contractual support for data and analytical services to optimize ICE operational support functions to enable mission success. This includes providing direct operational support for all aspects of screening and vetting, lead development, and criminal analysis as described below (see Background). It also includes, but is not limited to, conducting data extractions to identify unusual trends, data anomalies, and control breakdowns; identifying possible trends, patterns, and links to automate methods for detecting, monitoring, analyzing, summarizing, and graphically representing patterns of relationships between entities; identifying potentially criminal and fraudulent behavior before crime and fraud can materialize; and detecting and reporting elements of crimes involving the exploitation of the immigration and customs laws of the United States.

The Contractor shall use their own wide range of proprietary, commercial, and public data sources to include other commercial and government database sources to ensure optimal search capability to assist in determining whether criminals and/or entities are violating or attempting to violate U.S. immigration and customs laws or participating in government programs through potentially fraudulent misrepresentation, to run searches to return actionable intelligence, and to deliver comprehensive reports and products in response to requests and requirements.

Availability of the contracted services must be flexibly structured to adapt to changing priorities in the law enforcement continuum. During performance of the requirements identified, it is possible that the anticipated effort could potentially expand to increase the level of effort depending on plans to review and implement a centralized support initiative. This could require the level of effort to be an increase of the anticipated data and analytical services, or it could require scaling of analytical service personnel, such as adding new open-source researchers or increasing/decreasing the number of service personnel assigned.

Global data combined with analytical services is required agency wide. Over the last decade, ICE has used Operations Research Analysts and/or Data Scientists within the following entities to support criminal investigations and law enforcement operations:

- HSI Intelligence, including support to HSI Field Offices, the National Homeland Security Task Force and Protective Intelligence Unit.

- Computer and Operations Technology, including the Innovation Lab and Cyber Crimes Center.

- National Security Investigations Division, including the Student and Exchange Visitor Program.

- Global Trade Investigations, including the National Intellectual Property Rights Coordination Center and the Counter-Proliferation Mission Center.

- Countering Transnational Organized Crime Investigative Division, including the Cross-Border Financial Crimes Center, Document and Benefit Fraud Law Enforcement Unit, Work Site Enforcement Unit, and Undercover Operations Unit.

- HSI International (Support to Foreign Offices and VISA Security Program).

- ERO National Criminal Analysis and Targeting Center.

- ERO Law Enforcement Statistics and Analysis.

- OPR Protective Intelligence.

- OPLA National Security Law Division.

PERIOD OF PERFORMANCE

The period of performance of the BPA will include a twelve (12) month base period, four (4) twelve-month option periods, and one FAR 52.217-8 -- Option to extend services for one (1) six (6) month optional extension period.

The Government reserves the right to modify performance standards and/or metrics during the life of this contract, to ensure that the right outcomes are being assessed and that the performance standards are appropriate. Changes will be made via supplemental agreement within the change's clause.

The Government may terminate the performance of work under this contract in whole or, from time to time, in part if the Contracting Officer determines that a termination is in the Government's interest. The Contracting Officer shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date.

PLACE OF PERFORMANCE

The contractor shall be required to support investigations, operations, and initiatives throughout the United States.

Operational Footprint. Exact locations will be given upon award.

BACKGROUND

HSI's Guiding Principles of ***Data-Driven Support*** and ***Innovation*** and its goal to ***Optimize Operational Support Functions to Enable Mission Success***, are the drivers for this procurement. Technological innovation increases efficiency, decreases operational costs, enhances security, and actively promotes information sharing. Investigative techniques and equipment must be updated and effective in uncovering criminal activity to ensure investigative and intelligence resources operate most efficiently and have the greatest impact possible.

Agents, analysts and support personnel perform three lines of effort that require contract support for data and analytical services: Screening and Vetting, Lead Development, and Criminal Analysis.

- Screening and Vetting involves researching the names of individuals and entities in law enforcement and other databases to determine if they are threats to homeland security.

- Lead Development involves researching and analyzing individuals, entities and suspicious activities to develop and disseminate information (such as alerts, investigative leads and investigative referrals) about possible criminals and criminal activity. The process of developing and disseminating alerts is also known as targeting or tipping and cueing.

- Criminal Analysis is the comprehensive study of criminals and their networks, activities, associations, and impacts.

Every investigative and intelligence group, section, division and program routinely conducts at least one of these lines of effort and therefore would benefit from contract support that specializes in supporting these lines of effort

The need to uncover patterns in data using analytical methods and techniques enables the detection of criminal activities, criminal conspiracies, and criminal networks. Detection increases cooperation in investigations and leads to greater overall support for public safety, increases response rates, and gets results to decision makers much faster. The need to quickly analyze massive amounts of data along with current and developing conditions helps uncover fraud, risk, criminal activity, illicit finance, and terrorism patterns. By using data analysis methodology, law enforcement can analyze, model, and score massive amounts of data which makes it less challenging to capture and act upon critical information that will not only accelerate the criminal investigation process but also help to deploy agents and identify situations likely to escalate crime, fraud, risk, and terrorism acts/incidents, where needed.

The use of data (including access to unique proprietary datasets) combined with analytical services is needed to build on existing efforts to use data analytics to employ techniques like criminal network analysis to identify potential crime and fraud indicators, capture detailed data that would allow the detection of patterns and anomalies that could indicate criminal conspiracy and fraud, and mitigate fraud risks in compliance processes.

Agents and analysts routinely draw upon various government databases to gather and analyze leads regarding violation of immigration status, identify potential security or criminal threats,

and ensure full compliance with immigration laws. Data obtained for ICE programs are managed by the DHS Library Program Management Division as part of a DHS efficiency initiative. Although this is a massive collection of resources for homeland security partners, there is still a need for increased access to volumes of data content and information, with appropriate support from skilled researchers/analysts and data scientists to process this data and information.

GENERAL REQUIREMENTS

Our goal is to extract and aggregate data to identify possible trends, patterns, and links to criminal activity. The data and services must present data and content to be analyzed internally by both automation and trained analysts and agents with research support tools. It includes the ability to conduct, process, analyze, and report large volume bulk and batch queries along with a continuous monitoring and alert system that must be able to securely process and return information in a format compatible with agency systems and processes.

A wide range of proprietary, commercial, and public information data sources are required to ensure optimal search capability, run searches to return actionable intelligence, and deliver comprehensive reports in response to requests and requirements. This includes an online data analytics and investigative platform designed to streamline research and analysis and develop actionable insights by providing access to a vast array of public and proprietary data and linking law enforcement data.

Also required are data and analytical services with the ability to access, query, evaluate, process, integrate, analyze, and share the following required types of information and data to support criminal analysts, criminal investigators, and operational personnel utilizing both contractor tools and other government internal/external analysis resources:

- Business information
- Business associations
- Court records and information
- News and media reporting
- Social media (Facebook, X, Tik Tok, etc.) and web, including dark web
- Cyber information
- International trade data
- International travel data
- Transportation information
- Shipping information
- Advertising data and information
- Geolocation information (including license plate reader information)
- Public and proprietary records
- Law enforcement information
- Crime data
- Property records
- Commerce data
- Financial information
- Communications data

- Supply chain information
- Blockchain information
- Cryptocurrency data and information
- Education information
- Scientific research and development
- International patent information
- Other data and information that enables the analysis and investigation of criminals and criminal networks that exploit the customs and immigration laws of the United States.

ICE requires this data, as well as access to data through a team capable of using large scale data analysis platforms, obtaining/collecting from diverse sources, and automating data collection and analysis to present models that can repeat processes to quickly generate accurate predictions, reach goals, and monitor and report consistently. This combined service should develop data engineering models and products that can constantly and consistently leverage data as implemented automated solutions. This team should also be able to integrate effectively with ICE data teams, information systems, and data repositories.

ICE believes that it needs the following personnel to successfully implement this effort but is open to input by industry experts with suggestions on the most effective method for meeting this requirement:

Operations Research Specialists apply mathematical and analytical methods to help solve complex problems and make better decisions. They use techniques from operations research, statistics, and optimization to analyze data and develop models that improve efficiency and effectiveness. Typical responsibilities include:

1. **Problem Identification:** Identifying and defining problems within an organization that can be addressed using analytical methods.
2. **Data Collection:** Gathering relevant data from various sources to understand the context of the problem and potential constraints.
3. **Model Development:** Developing repeatable mathematical models and simulations.
4. **Optimization:** Applying optimization techniques to find the best possible solutions to problems, considering constraints and objectives.
5. **Analysis:** Analyzing the results of models and simulations to derive insights and recommendations.
6. **Implementation:** Working with stakeholders to implement solutions and monitor their effectiveness.
7. **Reporting:** Preparing detailed reports and presentations to communicate findings and recommendations to decision-makers.

8. **Collaboration:** Collaborating with cross-functional teams, including engineers, data scientists, and criminal analysts, to ensure solutions are feasible and aligned with organizational goals.
9. **Continuous Improvement:** Continuously refining models and methods to improve accuracy and effectiveness.

Data Scientists use scientific methods, processes, algorithms, and systems to extract knowledge and insights from structured and unstructured data. They combine expertise in statistics, computer science, and domain knowledge to analyze large datasets and solve complex problems. Key responsibilities include:

1. **Data Collection and Cleaning:** Gathering data from various sources and ensuring its quality by cleaning and preprocessing it.
2. **Data Analysis:** Applying statistical techniques and machine learning algorithms to analyze data and uncover patterns, trends, and relationships.
3. **Model Building:** Developing predictive models and algorithms to solve specific problems or make data-driven decisions.
4. **Visualization:** Creating visual representations of data findings to communicate insights to stakeholders effectively.
5. **Reporting:** Preparing detailed reports and presentations to share analysis results and recommendations with decision-makers.
6. **Collaboration:** Working with cross-functional teams, including business analysts, engineers, and domain experts, to understand requirements and deliver solutions.
7. **Continuous Learning:** Staying up to date with the latest tools, technologies, and methodologies in data science to improve their skills and the effectiveness of their work.

Data: ICE recognizes that there are companies within this industry that have created proprietary tools to perform the searches described in this requirement. Potential vendors shall provide a data dictionary in proposals outlining the types of data available within their proprietary database. To determine the effectiveness of proposals, we may provide a sample test case to be run within your system. Evaluators sign non-disclosure agreements when reviewing contractor proposals.

The National Security Clearance level could range from CONFIDENTIAL to TOP SECRET with access to Sensitive Compartmented Information.

The contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience equivalent to or greater than an undergraduate-level degree in quantitative field(s) (i.e. math, computer science, statistics, etc.). The contractor shall match personnel skills to the work or task assigned. The Contractor will submit contract employee's resumes to the call COR for the government for

review and concurrence of proposed personnel. The Contractor shall provide the necessary resources and infrastructure to manage, perform, and administer the contract.

The Contractor shall be aware that the Government and other contractors are engaged in similar and supporting work, requiring close cooperation. Contractors are expected to form a cohesive team to include the Government and other contractors, by fostering transparency and information sharing for successful task execution.

SPECIFIC REQUIREMENTS

- All personnel assigned to the contract will be U.S. Citizens.
- Access to multiple global content data combined with analytic professionals of which SMEs provide deep web data and global content collection and analysis.
- The Contractor's service will deliver comprehensive data and information in response to requests to validate/verify school, benefit, immigration, or other eligibility requirements.
- The Contractor, the Contractor's affiliates, and the Contractor's third-party agreement providers will allow search and detection capability to address vulnerabilities as a part of an effective criminal and fraud prevention program to verify individual and entity information when conducting initial certification and re-certification reviews.
- The Contractor's services will be provided by SMEs with access to the Contractor's various data sources and analytical tools. This includes an online data analytics and investigative platform designed to streamline research and analysis and develop actionable insights by providing access to a vast array of public and proprietary data and linking law enforcement data.
- The Contractor will deliver comprehensive reports in response to requests and requirements by using a risk-based evaluative approach to reflect evidence of misrepresentation to fraudulently acquire or maintain a method of exploitation of ICE programs.
- Search results directly connected to the target that also contain information related to the target's associates shall be included with all information returned to help visualize data to more efficiently direct investigative resources, and if necessary, take steps to mitigate risk through early warning techniques.
- A continuous monitoring and alert service that provides real-time data to support the identification and location of threats to public safety and/or national security. The continuous monitoring and alert system to track content from the available sources for specified new data and information enhances the mission to proactively scrutinize known or suspected crime, identify and disrupt terrorist criminal enterprises, prevent exploitation of the nation's immigration system and to expand the resource equities within the various law enforcement agencies and intelligence communities. The continuous monitoring and alert service must be able to monitor a million individuals or entities of interest.
- Focus on immigration and customs related investigations and operations relies heavily on linguistic capabilities to help prioritize, translate, and understand in a timely fashion the information to which it has access. Information of this value is often subtle or cryptic, which requires high standards of language proficiency and cultural knowledge. In some cases, international information may require the ability to translate a specific language. For example, HSI requires the capability to transcribe/translate the Mandarin language.

- HSI's Investigative Programs Division (IPD), National Targeting Center (NTC), National Intellectual Property Rights (IPR) Coordination Center, and National Security Investigations Division (NSID) Student Exchange and Visitor Program (SEVP), require immediate enhanced ability to identify, disrupt, and dismantle organizations involved in the exponential growth of internet and global online fraud and crime posing a threat to national security. Particularly, the HSI IPD, and IPR, handle commercial fraud investigations while the NSID SEVP is focused on general school fraud investigations; all these entities recognize that fraud leads to many violations that fall under a larger scheme involving other HSI program areas focused on human smuggling and trafficking, narcotics/drugs, gangs, trade and financial crimes.
- HSI has a law enforcement sensitive requirement to support undercover operations.
- ICE requires support protecting high profile officials, personnel, operations, facilities, and information.
- Requests, reports and products developed by the contractor must be available in a format that can be shared within ICE and released to ICE's partners.
- ICE requires that the contractor works within the agencies various analytics platforms to expand the agency's ability to conduct data extractions to identify unusual trends, data anomalies, and control breakdowns. In addition, emphasis will be placed on identifying possible trends, patterns, and links to automate methods for detecting, monitoring, analyzing, summarizing and graphically representing patterns of relationships between entities identifying potentially criminal, threat, and fraudulent behavior before it can materialize. The combination of criminal, security and fraud investigation expertise and technological skills provides an integrated approach to closing immigration and customs related vulnerabilities that could pose substantial risks to homeland and national security (including the diversion of sensitive technology, materials, or information).
- All data products will be presented for review and analysis to agency criminal analysts and/or government leads. Search and detection results directly connected to a target which may contain information related to the target's associates shall be included with all information returned to help visualize data to more efficiently direct investigative resources, and if necessary, take steps to mitigate risk through early warning techniques.
- Contract personnel must be able to access and develop tools and systems for screening and vetting, lead development and criminal analysis including producing network analysis, link analysis, call-chain analysis, supply chain analysis, market models, financial analysis, impact assessments, criminal profiles, crime mapping, geospatial analysis, forensics, and other forms of advanced analysis to identify and address threats to homeland security.

TASKS

ICE requires data, as well as access to data through a data team capable of using large scale data analysis platforms, obtaining/collecting from diverse sources, and automating data collection and analysis in order to present models that can repeat processes to quickly generate accurate predictions, reach goals, and monitor and report consistently. The combination of tools and services will deliver data engineering models and products that can constantly and consistently leverage data as implemented automated solutions.

It is expected that the data sets include SMEs able to provide/perform the expected data access, data processing, and data research and analysis activities. The SMEs are tailored to the client requirements (individual calls) and may include:

OPERATION RESEARCH SPECIALIST (DATA ANALYST) TASKS MIGHT INCLUDE:

- Identify, coordinate, harvest, and expose relevant data sources across multiple domains and classification levels for the purposes of screening and vetting, lead development and criminal analysis to support investigations and operations
- Identify the various problem sets within ICE analytics to identify support gaps
- Gather input and requirements for methodology development, modification, and tailored mission support
- Provide on-site assistance, instruction, and education to ICE personnel including but not limited to utilizing lessons learned, and knowledge from ICE AORs, TTPs, operations and mission priorities to enable and ensure effective use and augmentation of data capabilities
- Collaborate with capability developers to enable customization of features and functionality to meet ICE requirements
- Enable a robust community of users by facilitating sharing of analysis methods and use cases between ICE field personnel, ICE HQ analysts, and interagency partners as applicable
- Foster collaboration among mission partners by establishing a Point of Contact (POC) and coordination point for communities of interest
- Facilitate collaboration and sharing of data and threat information
- Draft agreements and tailor documentation in the form of MOAs, MOUs, Commercial and other agreements to support data ingestion.
- Utilize agency and industry standards to evaluate the validity, accuracy and reliability of a broad array of and high volume of information for translation into intelligence relevant to ICE
- Initiate contact with key personnel, fellow intelligence analysts and experts to validate and ascertain the reliability and urgency of information
- Monitor intelligence trends to anticipate and recommend operations requirements
- Maintain operational relationships with ICE personnel and facilitate a collaborative effort

DATA SCIENTIST SPECIFIC TASKS MAY INCLUDE:

- Coordinate and foster collaborative working relationship between ICE and mission partner personnel on all projects
- Identify, coordinate, harvest, and expose relevant mission-partner data sources across multiple domains and classification levels for ingestion into ICE
- Identify mission-partner priorities and problem sets to identify support gaps
- Gather input and requirements for methodology development, modification, and tailored mission support
- Enable a robust community of users by facilitating sharing of analysis methods and mission IT use cases between partner-site personnel, ICE analysts, and personnel at other partner sites

- Facilitate collaboration and sharing of data, threat information, and intelligence analysis between ICE and the mission partners
- Deploy as needed to support field requirements for training
- Provide increased support for data ingestion and enrichment, data sciences, integration and fusion on demand in response to new and expanding requirements, global events, mission partner requirements, etc.

DELIVERABLES

All deliverables are to be provided electronically via electronic transfer or email regarding the specified due dates in their final format. All deliverables require review and acceptance by the appropriate Government representative (Call COR/ACOR/PM) and there shall be no proprietary formatted documentation. All documentation (deliverables, etc.) developed by the Contractor shall become the sole property of the U.S. Government and can be utilized IAW FAR 52.227-17.

Documentation shall not include brands, logos or other marks identifying ownership or authorship besides the Government. In fulfillment of this contract, the Contractor shall be responsible for maintaining and reporting accurate and current technical and project management reports. Calls may require participation in routinely scheduled status meetings and reviews as agreed in the order. In addition to the delivery descriptions cited below, all deliverables shall also remain consistent with the DHS ICE SLM and MD4300 Security documents. Other deliverables may be identified and added in the event of changing mission requirements or new initiatives and tasks requested by other Government entities and stakeholders.

Supervisory Program Manager/Call Program Managers

The Contractor shall provide a Supervising Program Manager (SPM) who shall be responsible for all Contractor work performed under this SOO. The SPM will be a single point of contact for the Office of Intelligence and manager of this larger contract effort. Costs for this SPM will be included in an individual call for the HSI/Office of Intelligence.

The SPM will be responsible for providing the following Deliverable:

1) A comprehensive report of all monthly invoices provided to Call CORs.
   To include a consolidated report submitted to the Office of Intelligence COR with all contract work hours/activities including:
   - Name of Individual Contract Employee
   - Assigned Call Number
   - Dates/Hours Worked (By Call if assigned to multiple.)
2) Individual Call Reports with Monthly Invoices
   To include the following for each Call with all contract work hours/activities including:
   - Name of Individual Contract Employee
   - Assigned Call Number
   - Dates/Hours Worked in support of the effort
   - Additional information may be included in Call SOOs

The Contract may assign individual PMs to calls at the expense of and request of the originating office. Individual calls must have an assigned COR/ACOR and a government technical representative if different from the COR. The name of the PM, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the PM, shall be provided to the Government as part of the Contractor's proposal. Each individual call is to be billed independently to the attention of the assigned COR. The contract COR assigned to this larger effort is not responsible for managing the administrative activities of individual calls.

The PM/SME shall be available to the call COR/ACOR/Technical Representative via telephone between the hours of 0830 and 1700 local time, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 8 hours of notification. Individual Calls may alter this timeframe if their mission requires a more expeditious respond. The PM/SME shall meet with the COR/ACOR/Technical Representative upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place telephonically or at a location mutually agreed to between the COR/technical representative and PM/SME.

The PM/SME shall ensure that: (1) the goals and objectives of the project and (2) problem resolution and customer satisfaction are accomplished within prescribed timeframes and funding parameters. Key duties include planning, organizing, directing, and controlling the project to ensure all contractual obligations are fulfilled, quality standards are met, and associated expectations of performance achieved. Other duties include developing schedules, reviewing work discrepancies and managing contractor staff. The PM/SME shall have/maintain a level of classification of Top Secret with eligibility to Sensitive Compartmented Information (SCI).

Project Plan

The Contractor shall develop a Project Plan outlining resources, activities, and milestones necessary to accomplish the work specified in each call. Technical activities in the schedule shall be at a level of detail sufficient for the Contractor to manage the task. The Contractor shall amend the Project Plan schedule, whenever a modification to the contract occurs that affects the Project Plan. The Contractor shall provide the final plan within forty-five (45) calendar days after award. The Project Plan shall also include a critical milestone schedule (e.g.: staffing, logistics). The plan shall describe the planning and control system for this program. The plan shall include:

- A description of the procedures to be used for measuring and reporting progress.
- A discussion of internal schedule control.
- A schedule showing milestone events.
- An approach for controlling the data model design and delivery
- A description of the techniques used to identify, monitor and control technical and program risks.

Monthly Activity/Status Reports

The Contractor may be asked to provide call monthly progress reports to ensure that its expenditure of resources is consistent with and shall lead toward successful completion of all

tasks within projected cost and schedule limitations. Each call may include requests for Monthly Activity/Status Reports. These reports may require detailed 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 milestone schedule. The report may include all activities and scheduling updates. Each call will outline the individual requirements of that office.

Project Assignment - Deliverables Ad Hoc, Batch and Data Extraction/Model Reporting
The Government will assign contract personnel projects ranging in size and complexity as described throughout their calls. Assigned personnel will work with designated points of contact to understand and document the requirements of the project. Calls may request a variety of data models, data extractions, or other ad hoc data reports pertinent to their requirements. Urgent/Emergency, routine and non-routine queries and reports will be run, as determined and as requested.

Project assignment deliverables may include one or more of the following:

1. MS Power Point, MS Word, MS Excel, graphics or similar reports describing the findings of the data analysis
2. Github README documents and Confluence pages.
3. Web Based user interface dashboards/tools both custom and leveraging tools such as Kibana, available within the ICE environment.
4. Proof that data was loaded into a designated system. This proof would generally be in the form of screen shots but could be provided in other formats.
5. Machine Learning models.
6. Scripts or other code which accomplishes the objective of the project assignment.

The data models should demonstrate and deliver varied levels and ranges for data extraction, data aggregation, and data visualization. It is expected that the data sets include the best leads possible for agents and analysts. The data products should reflect source information, holdings, legal, and access information for the data sets to include, but not limited to: State Identification Numbers; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; property information; payment information; public court records; address data; Individual Taxpayer Identification Number (ITIN) data; and employment records. The Contractor shall use the Government-provided Product Backlog Repository and defect management tool, currently JIRA, to document and track user story and task progress related to project assignments. Good agile development processes should be adopted, and user stories/tasks should be decomposed at a level where the government can clearly see the progress that is being made on project assignments. As a general a rule, a single Jira user story/task should never contain more than two days of work. If the user story/task is larger than this, it should be split into multiple sub-tasks.

The Contractor shall store and manage all system configuration settings, development code and documentation in the ICE Approved Software Configuration Management (SCM) system, currently GitHub Enterprise.

The Contractor shall document operational tasks and Standard Operating Procedures (SOPs) in an ICE Approved knowledge management portal, currently Confluence.

Table 1. Schedule of Deliverables

Deliverable No.	Description	Frequency	Due Date
1	**Draft Project Management Plan:** The Contractor will prepare and submit a Draft Project Management Plan to document major milestones, review points and delivery dates for the initiative.	Once per Call.	Initial draft 30 days after award date; final due 45 days after award; electronic format using Microsoft Suite Products or .pdf
2	**Monthly Activity/Status Report:** The Contractor will provide a monthly activity report documenting the progress toward each task deliverable, identifying problems encountered in areas of risk, status of task, personnel changes and other information pertinent to completion and identified by the Call COR or Project Manager.	Monthly is typical, however, they may be requested at different intervals in individual calls.	10th working day of the month; electronic format using Microsoft Suite Products or .pdf
3	**Intelligence Request Responses and Reports:** The Contractor will provide various types of responses and reports based on the client's description and desired timeframe for delivery	As requested.	Electronic format using Microsoft Suite Products or .pdf -URGENT/EMERGENCY - delivery: no more than 1 day -ROUTINE - delivery: no more than 3 days -NON-ROUTINE - delivery: as established by mutually agreed upon deliverable date(s) with the COR and/or GTM

MEETINGS

Post-Award Orientation Conference

The Contractor shall commence work on the first day of the period of performance at the Contractor's facility if personnel are not able to obtain personal identity verification (PIV) and/or security clearance access for the designated site location. The Post Award Orientation Conference shall be coordinated with the Contracting Officer and held no later than 15 days after award. The Contractor shall participate in a post-award conference for the purposes of making

introductions, coordinating security requirements, discussing schedules, prioritizing SOO requirements.

SPM, PM/SME, CO, COR/ACOR and Government Task Monitor (GTM) Progress Meetings
The CO, COR/ACOR and GTM, as appropriate, will meet periodically or participate in teleconferences to review contract performance, progress, and resolve technical issues. Minutes of the meetings/teleconferences, with action items identified, shall be documented by the Contractor and provided to the COR no later than 72 hours after meeting.

INSPECTION AND ACCEPTANCE

All reports, documentation, and task deliverables shall be reviewed and accepted by the Government. The Call COR/ACOR will monitor compliance and report to the Contracting Officer.

PUBLIC & COMMERCIAL SOURCE SEARCHES AND SEARCH RESULTS

The Contractor shall return to ICE from publicly available and commercial sources available to the Contractor, any information that identifies targets as well as affiliated organizations, entities, and relationships through which fraud and/or threat can be derived. Results will be electronically transferred via encryption and through official ICE email addresses.

Search results directly connected to the target that also contain information related to the target's associates shall be included with all information returned to ICE. Upon exhaustion of initial search information, ICE may request that the Contractor conduct a follow-up search and return of information that includes any publicly available information about the target's associates, such, but not limited to family members, friends, or co-workers, through which a location of the target may be derived.

Publicly Available Sources
Only searches of Internet and social media sites and facilities that are open to the general public (open source) in the U.S. and in foreign jurisdictions are permitted. Searches are to include social media profiles on a variety of social media sites, including, but not limited to Facebook, LinkedIn, Twitter, etc. The Contractor shall search only publicly accessible information, including social media profiles.

The Contractor and Contractor personnel must adhere to the following requirements when obtaining information from public sources in fulfillment of their duties under the contract:

1. Obtaining Information from Unrestricted Sources. When conducting searches the Contractor may obtain information from publicly accessible online sources and facilities under the same conditions that 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, 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. Additionally, email must be handled in accordance with FIPS 140-2, NIST SP 800-175B, and DHS 4300A Policy Encryption Standards.

7. International Issues. Unless gathering information from online facilities configured for public access, the Contractor should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever an item or person is located abroad, the Contractor should notify ICE, and ICE law enforcement personnel should follow ICE's policies and procedures for international investigations.

8. Email must be encrypted using end-to-end security. End-to-end security means that the entire message is encrypted from sending device to receiving device. Both devices must use appropriate FIPS 140-2 validated encryption. The contractor agrees to ensure that proper authentication and encryption mechanisms are implemented, so as toto ensure data integrity, confidentiality, and availability.

The Contractor shall not maintain any data, including the list of targets provided by ICE and search results provided to ICE after the analysis is complete, nor shall the Contractor maintain any data on behalf of ICE 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 ICE for any outside commercial purpose.

RELEASE OF INFORMATION

Contractor access to proprietary and Privacy Act-protected information is required under the SOO. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the Privacy Act of 1974, and the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS. Contractor and subcontractors shall not hold any discussions or release any information relating to this contract to anyone not having a

direct interest in the performance of this contract, without written consent of the Contracting Officer (CO) and Call Contract Officer's Representation (COR). This restriction applies to all news releases of information to the public, industry or Government agencies, except as follows: Information for actual or potential subcontractors or other individuals necessary for Contractor's performance of this contract. Contractor and subcontractors shall not issue advertisements about projects performed under this task without government review and approval. For the purposes of this paragraph, advertisement is considered to be Contractor-funded promotional brochures, posters, tradeshow handouts, world-wide-web pages, magazines, or any other similar type promotions.

NON-DISCLOSURE

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of these tasks and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of these tasks. Contractor personnel are required to sign Non-Disclosure statements (DHS Form11000-6).

All information, including documents, workflows, products, training materials, or programs, created in support of ICE, at the request of the ICE management or staff, or generated as a result of this contract, which contain or are derived from U.S. Government proprietary data are the sole property or will become the property of ICE and the U.S. Government.

All material, code or products developed under this contract which do not contain proprietary U.S. Government information are governed by the terms of FAR 52.227-17. Special care and discussion shall be taken surrounding Machine Learning Models which may be developed within this contract as often the algorithm may be subject to FAR 52.227-17 but the trained model would be the sole property of ICE and the U.S. Government if it was trained using U.S. Government proprietary information.

HOURS OF OPERATION

Contractor employees shall generally perform all work on site with the Call holder between the hours of 0830 – 1700 local time (Hours may vary per individual Calls), Monday through Friday (except Federal holidays) and are expected to work a 40-hour work week. However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOO.

Federal Holidays in each calendar year identified as follows:

New Year’s Day
Martin Luther King’s Birthday
Washington’s Birthday
Memorial Day
Juneteenth Day
Independence Day
Labor Day

Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

The above identification of Federal Holidays is provided to inform the contractor of when the facilities identified under "place of performance" will be closed. Other non-workdays will occur if there is an executive order closure, bad weather days, or building closures due to emergency repairs, inhabitable conditions or threat of possible security.

TELEWORK/REMOTE WORK

Telework/Remote Work is not authorized under this agreement regardless of what individual calls may indicate. Contractors must report to the government facility indicated in each Call.

The Supervisory Program Manager (SPM) is the only exception to this requirement and may work from the contractor's facility.

In the event of such extreme emergency case; natural, man-made or otherwise, whereas government closure is required, situational and/or Episodic telework by contractor staff is not permitted.

ORGANIZATIONAL CONFLICT OF INTEREST

The Contractor warrants that, to the best of its knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in Federal Acquisition Regulation (FAR) Subpart 9.5, or that the Contractor has disclosed all such relevant information in writing to the Contracting Officer (CO).

The Contractor agrees that if an actual or potential organizational conflict of interest is discovered after the award, the Contractor shall make a full disclosure in writing to the CO no later than three working days after discovery. This disclosure shall include a description of actions that the Contractor has taken or proposes to take, after consultation with the CO, to avoid, mitigate or neutralize the actual or potential conflict.

The Contractor further agrees to insert provisions, which shall conform substantially to the language of this clause, including this text, in any subcontract or consultant agreement hereunder.

<u>Remedies</u>
ICE may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an organizational conflict of interest. If the Contractor was aware or should have been aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the CO, the Government may terminate the contract for default, debar the

Contractor from Government contracting or pursue such other remedies as may be permitted by law or this contract.

DATA USE, DISCLOSURE OF INFORMATION AND HANDLING OF SENSITIVE INFORMATION

The Contractor shall maintain, transmit, retain in strictest confidence, and prevent the unauthorized duplication, use, and disclosure of information. The Contractor shall provide information only to employees, Contractors, and subcontractors having a need to know such information in the performance of their duties for this project.

Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer.

If public information is provided to the Contractor for use in performance or administration of this effort, the Contractor except with the written permission of the Contracting Officer may not use such information for any other purpose. If the Contractor is uncertain about the availability or proposed use of information provided for the performance or administration, the Contractor will consult with the COR regarding use of that information for other purposes.

The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each offeror or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor, which is of such a nature that its dissemination or use, other than in performance of this effort, would be averse to the interests of the Government of the Government and/or others.

Contractor and/or Contractor personnel shall not divulge, or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the CO. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort.

TRAVEL

Travel may be required. Individual Calls may include Travel and provide funding for travel of contractors as needed. Travel to sites outside of the Washington, DC area and to government facilities, if required, in conjunction with the performance of contract shall be in accordance with the Federal Travel Regulation. The Contractor must submit travel requests to the assigned COR/ACOR no less than 21 days in advance with the appropriate pre-travel cost estimates. Travel requests must be approved in writing by the Contracting Officer Representative (COR) prior to travel.

All travel required by the Government outside a 50-mile radius of the Washington, D.C. metropolitan area shall be reimbursed to the Contractor in accordance with the Federal Travel Regulations. but shall not be performed without prior written approval of the COR or the CO. The Contractor shall be responsible for obtaining COR approval for all reimbursable travel in advance of each travel event. Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodation available during normal business hours.

The Contractor shall not be reimbursed for transportation expenses of assigned personnel for local commuting and parking between their place of residence and their place of work. The Contractor shall not be reimbursed administrative fees for processing travel claims.

GOVERNMENT FURNISHED INFORMATION

The Government will furnish the necessary network access and accounts or shall sponsor the contractor in setting up the necessary accounts to ensure communication with all necessary Offices. Each Call COR will provide all documentation necessary for completion of the requirements. GFI including ICE policies, templates, standard operating procedures (SOPs), guidance documents, and other promulgated directives are contained in the ICE Non-Classified Local Area Network (NLAN) and various SharePoint sites.

GOVERNMENT FURNISHED PROPERTY and OTHER RESOURCES

Each Call COR/PM will provide a workspace within a DHS/ICE facility. The Government will not provide parking at work locations. The Contractor may request information technology support. All materials provided by the Government are the sole property of the U.S. Government, Department of Homeland Security and must be handled as UNCLASSIFIED, FOR OFFICIAL USE ONLY; or as appropriately classified. All Government furnished property will be returned upon completion of the task.

The government will furnish the contractor at a government facility with access to the following equipment in support of this contract:

- Workspace
- Stationary supplies
- Photocopier
- Printer
- Scanner
- Computer or laptop
- Containers for storage of documentation/reference
- Audio visual equipment
- Phone/facsimile

Communications: The contractor will be provided with access to the ICE LAN network and an email address. Workspace with access to unclassified ICE network connections or other networks as needed to fulfill the mission requirement.

Government Furnished Information and Support: The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the COR and Contracting Officer.

FAR Clauses Incorporated by Reference

52.204-2 Security Requirements

52.224-1 Privacy Act Notification (Apr 1984)

52.224-2 Privacy Act (Apr 1984)

52.224-3 Privacy Training – *Alternate I (Jan 2017)*

52.227-11 Patent Rights -- Ownership by the Contractor (May 2014)

52.227-17 Rights in Data – Special Works (Dec 2007)

SAFEGUARDING GOVERNMENT PROPERTY

If the work under this contract requires that the contract employees have access to classified, confidential, proprietary, sensitive, personal, business, technical, or financial information (property) belonging to the Government or to other private parties performing or seeking to perform work for the Government, no employee of the Contractor shall be authorized to read, photocopy, remove, or otherwise appropriate such information for his/her own use or disclose such information to third parties unless specifically authorized in writing by the CO. Violations of this policy may result in Contractual actions being taken, up to and including termination for default. Additionally, the Government may pursue any legal remedies at its disposal if the unauthorized use of the information/property is prosecutable under law.

UNAUTHORIZED COMMITMENTS (FAR 1.602.3)

The COR is designated by the Contract Officer (CO) to perform as a technical liaison between the Contractor's management and the CO in routine technical matters constituting general program direction within the scope of the contract. Under no circumstances is the COR authorized to effect any changes in the work required under this contract whatsoever or enter into any agreement that has the effect of changing the terms and conditions of this contract or that causes the Contractor to incur any cost. In addition, the COR will not supervise, direct or control Contractor employees.

Notwithstanding this provision, to the extent the Contractor accepts any direction that constitutes a change of this contract without prior written authorization of the Contracting Officer; costs incurred in connection therewith are incurred at the sole risk of the Contractor and if invoiced under this contract will be disallowed. On all matters that pertain to the contract terms, the Contractor must communicate with the CO.

Whenever, in the opinion of the Contractor, the COR requests efforts beyond the terms of the contract, the Contractor shall so advise the CO. If the COR persists and there still exists a disagreement as to proper contractual coverage, the CO shall be notified immediately, preferably in writing. Proceeding with work without proper contractual coverage may result in nonpayment or necessitate submittal of a contract claim.

ACCESSIBILITY REQUIREMENTS

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-
220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards
36 CFR 1194.21 Software Applications and Operating Systems applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required

1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offers telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions
Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements
36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

PRIVACY AND RECORDS REQUIREMENTS

The data processed within ICE shall be considered federal law enforcement sensitive, and, therefore, cannot be used to solicit or benefit other work by the contractor. All records received, created, used, and maintained by the contractor for this effort shall be protected as sensitive data, in accordance with government laws, to include the FAR, Part 24, Protection of Privacy and Freedom of Information, and shall be returned and provided to the government upon contract completion.

All data created for government use and delivered to or falling under the legal control of the government are federal records and shall be managed in accordance with records management legislation as codified at 44 U.S.C. Chapters 21, 29, 31, and 33, the Freedom of Information Act

(5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a), and shall be scheduled for disposition in accordance with 36 CFR 1228.

As prescribed in FAR 24.104, under the Privacy Act Notification Clause (Apr 1984), the contractor shall comply with clauses 52.224-1 and 52.224-2. Clause 52.224-1 specifically states that when the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the contractor will be required to design, develop, or operate a system of records on individuals to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.
Clause 52.224-2

The contractor agrees to-

Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies the systems of records and the design, development, or operation work that the contractor is to perform

a. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without solicitation, when the work stated in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

b. Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which require the design, development, or operation of such a system or records.

In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

a. "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

b. Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

c. "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

All contractor employees for this effort will also be required to sign a Non-disclosure statement, Acknowledgement and Agreement Handling Sensitive Government Data and Other Government Property and are subject to the security requirements of the SOO. This form will be signed prior to beginning work for this effort.

PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment. Government information shall always remain within the confines of authorized Government networks. The Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities.

Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.
As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights

Except as stated in the Statement of Objectives and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements

If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOO required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

REQUIRED SECURITY LANGUAGE FOR CONTRACTS REQUIRING CONTRACTOR EMPLOYEES ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION

SECURITY REQUIREMENTS

GENERAL

Performance under this agreement will require access to Classified National Security Information (NSI) by contractor employees. Contract agreement # XXXXXXXX requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) may access Classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the *National Industrial Security Program Operating Manual (NISPOM)* for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at an ICE or other Government Facility, it will abide by the requirements set by the agency.

In conjunction with acquisition XXXXXXXX the contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 2-1.

No person shall be allowed to begin work on contract XXXXXXXX and/or access sensitive information related to the contract without ICE receiving clearance verification from the Facility Security Officer (FSO). ICE further retains the right to deem a contractor employee ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a Continuous Evaluation Program. Any action taken by ICE does not relieve the Contractor from required reporting of derogatory information as outlined under the NISPOM.

The FSO will submit a Visit Authorization Letter (VAL) through the Contracting Officer's Representative (COR) to psu-industrial-security@ice.dhs.gov for processing contractor employees onto the contract. The clearance verification process will be provided to the COR during Post-Award conference. Note: *Interim TS is not accepted by DHS for access to Top Secret information. The contract employee will only have access to SECRET level information until DoD CAF has granted a final TS.*

See BACKGROUND INVESTIGATIONS paragraph below for processing of contractor employees who will not require access to Classified NSI in support of this agreement.

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding or terminating unescorted 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)

BACKGROUND INVESTIGATIONS (Process for personnel not requiring access to classified information):

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 Personnel Security Unit. 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 Contracting Officer Representative (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 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 contractor employee was born abroad. If applicable, additional form 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 applicant has not had a break in service of more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

Required information for submission of security packet will be provided by OPR-PSU at the time of 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 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 121-01-007-001. 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.

TRANSFERS FROM OTHER DHS CONTRACTS (Unclassified support position):

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.

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 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 OPR-PSU will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of contractor employees.

REQUIRED REPORTING:

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 responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contractor 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 the 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.

The contractor is required to report certain events that have an impact on the status of the facility clearance (FCL) and/or the status of a contractor employee's personnel security clearance as outlined by *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter1-3, Reporting Requirements. Contractors shall establish internal procedures as are necessary to ensure that cleared personnel are aware of their responsibilities for reporting pertinent information to the FSO and other federal authorities as required.

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.

Contractors shall provide all employees supporting contract XXXXXXXX proper initial and annual refresher security training and briefings commensurate with their clearance level, to

include security awareness, defensive security briefings. (*National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 3-1. The contractor shall forward a roster of the completed training to the COR on a quarterly basis.

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 their 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).

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, 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, 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).