

**Statement of Work for
HSARPA Border Enforcement Analytics Program APEX
BIG DATA ENVIRONMENT (BDE)**

**U.S. Department of Homeland Security
Science and Technology Directorate**

I. BACKGROUND

1.1 The U.S. Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Directorate of Science and Technology (S&T) is tasked with researching and organizing the scientific, engineering, and technological resources of the United States and leveraging these existing resources into technological tools to help protect the homeland. The Homeland Security Advanced Research Projects Agency (HSARPA) mission is to facilitate revolutionary research and development to transform and improve homeland security mission space through rapid prototyping, demonstrations, technology transition, test and evaluation and commercialization of new and highly effective capabilities for the homeland security enterprise.

1.2 This Statement of Work (SOW) delivers research and development support to Immigration and Customs Enforcement Homeland Security Investigations (ICE-HSI) through the development and transition of a Big Data Environment (BDE).

II. SCOPE OF WORK

The scope of work in the base year will be focused on developing capabilities for a single domain of investigations that will be disclosed to the contractor on contract award.

2.1 DHS S&T has partnered with ICE/HSI on the Border Enforcement Analytics Program (BEAP) Apex program. The goal of the program is to deliver next generation data storage and analytical capabilities to ICE in order to assist HSI agents in their investigative work.

2.2 This Statement of Work (SOW) addresses transition deliverables for the BEAP Apex project by creating an architecture and analytic support environment that can host analytical tools and data stores provided by DHS S&T at ICE.

2.3 Through this SOW, DHS seeks to create a development and testing computing cluster at ICE to begin the process of integrating big data analytics and storage capabilities into the ICE operational development environment. This development and testing compute cluster in the operational environment is expected to align with ICE privacy and information assurance policies and regulations regarding the creation and maintenance of systems technology. The resulting computing cluster and computing environment will be known as the ICE Big Data Environment (BDE), and will become a component of the Authoritative ICE Data Warehouse (AIDW), an RDBMS solutions that is now under development.

III. TASKS – BASE PERIOD OF PERFORMANCE

3.1 The contractor shall work with a government prototype, made of commercial server hardware and software, to create and maintain a developmental computing cluster in a development and test environment within the ICE IT boundary and will be required to:

3.1.1 Create, configure, maintain and support various commercial implementations of open source Hadoop File System (HDFS) and other related source software products that utilize the Hadoop platform.

3.1.2 Reconfigure (e.g. increase and/or decrease the number of nodes) the cluster as part of supporting server configurations or virtual machines effectively and efficiently.

3.1.3 Establish, maintain and patch versions of the HDFS and software associated with HDFS as required to maintain proper function and system security requirements in accordance with system security guidance as provided by the ICE Information Systems Security Officer (ISSO) via the COR.

3.2 The contractor will be required to integrate and maintain analytics and visualization tools that directly access storage systems such as HDFS, MongoDB, and RDBMS systems. This may include additional coding and development in a common programming language (e.g. C, C++, Java, Python, etc.) to properly integrate analytics and visualization tools and software that provides new lead development capabilities for analysts, agents and investigators. Such integrations may involve the utilization of Ozone Widget Framework

~~3.3 The contractor is required to provide a methodology and analytical approach for migrating the ICE Big Data Environment (BDE) to a Production environment at ICE. The contractor is expected to carry out the work required to migrate the BDE system from a development and test system to a production system environment that is fully compliant with all ICE and DHS protocols such as FISMA, FIPS, DHS Privacy and other compliance standards.~~

3.4 The contractor is required to develop the Hadoop cluster, and any bolt-on analytic and visualization tools, in accordance with IT regulations, best practices, and requirements as provided by the ICE Office of the Chief Information Officer via the COR. This will include, but not limited to:

3.4.1 Integration of the Hadoop cluster and visualization tool with authentication and authorization requirements provided by the BDE Information System Security ISSO (via the COR) for development and production systems that access operational networks.

3.4.2 Create the development and production instances of BDE in alignment with regulations provided by the BDE ISSO and the OCIO Information Assurance Division (via the COR), including requirements to have the system attain Authority to Operate (ATO) and Certification and Accreditation (C&A) of the system.

3.4.3 Ensure that all hardware and software is compliant with ICE security requirements, including but not limited to:

3.4.3.1 Development of security controls, in accordance with DHS/ICE configuration guides, for all operating systems and software residing on IRMNET.

3.4.3.2 Maintenance and production of security and access logs as required by the BDE ISSO.

3.5 The contractor is expected to administer the BDE system including the implementation of user rights and access management for the Hadoop cluster for DHS users for the duration of the contract.

3.6 The contractor is expected to develop a web-based user interface to the Hadoop cluster that will allow access to an undefined number of visualization tools from a consolidated dashboard.

3.7 ~~The contractor will be required to architect and model all data being uploaded into the BDE system. This will include, but not limited to:~~

3.7.1 ~~Creation of a data model for data sets that ICE intends to upload into BDE to ensure accuracy when accessed by operational units at ICE.~~

3.7.2 ~~Creation of a model that clearly depicts the data architecture that will be associated with the BDE system.~~

3.8 The contractor will be required to test, develop and integrate Extract, Transform and Load (ETL) tools into the BDE system.

3.9 ~~The contractor will be expected to support Test and Evaluation (T&E) activities carried out by ICE and DHS S&T for BDE system.~~

3.10 ~~The contractor shall develop an interface between BDE and the Authoritative ICE Data Warehouse (AIDW), in order to import and export data to/from an SQL to a NoSQL data store.~~

3.11 ~~The contractor shall provide Database Administrator functions for the Hadoop cluster, and have the knowledge and ability to address any system outages or other discrepancies associated with the cluster.~~

3.12 The contractor shall participate in planning and execution of tasks that will collaborate with ICE to develop the BDE capabilities and accommodate evolving requirements, such as the ingestion of new data sources, utilizing Agile or other relevant development processes.

3.13 ~~Project Plan/Schedule. Within 30 days after award, the contractor shall provide a project plan and schedule that consists of:~~

3.13.1 ~~Each task identified in Section III of this SOW.~~

3.13.2 ~~Individual work elements necessary in order to complete each task.~~

3.13.3 Milestones associated with each work element and each task that demonstrates the completion of the SOW within the period of performance of the contract.

3.14 Technical Status Reports. The contractor shall provide monthly technical status reports to the COR by the 15th of first full month following award and thereafter on the 15th of each month during the period of performance of the contract. The monthly report shall be electronic and in a format agreed to by the COR, to be established after award. This report shall include:

3.14.1 Period being reported.

3.14.2 A narrative of all contractor work performed during the previous month, including:

3.14.2.1 A description and assessment of technical progress;

3.14.2.2 Status of each task listed in Section III of the SOW with a description and overview of items and activities completed in the reporting period and planned activities for the next reporting period;

3.14.2.3 Identification of any risks and mitigation plans for those risks including any challenges and the contractor's plans to overcome those challenges; and

3.14.3 Updated Project Schedule. The contractor shall provide an updated project schedule clearly depicting any schedule changes from the previous submission.

3.15 Financial Reports: The contractor shall provide monthly financial status reports by the 15th of first full month following award and thereafter on the 15th of each month during the base period of performance to the Contracting Officer and the COR. The monthly report shall be electronic and in a format agreed to by the Contracting Officer, to be established after award.

3.15.1 The first report submitted shall include:

3.15.1.1 The obligated amount of the contract; and

3.15.1.2 A spend plan outlining how the contractor will, by task identified in Section III of the SOW, spend the obligated amount of the contract.

3.15.2 Each subsequent report shall include:

3.15.2.1 The obligated amount of the contract;

3.15.2.2 An updated spend plan showing the original spend for each task identified in Section III of the SOW as well as any changes, clearly delineated, to the original spend plan;

3.15.2.3 Total costs incurred during the previous reporting period;

3.15.2.4 Total costs incurred the period being reported;

3.15.2.5 Estimate of percentage complete (based on work completed, not funds spent) of each task identified in Section III of the SOW; and

3.15.2.6 A breakdown by cost element (e.g., labor, materials, indirect costs, other directs, travel, etc.) of costs incurred during the reporting period.

3.16 Quarterly presentation (as designated by the COR) to the Joint Border Enforcement Analytics Program (BEAP) Steering Group regarding the status of the ICE Big Data Environment (BDE). The presentation shall consist of a summary of the design, implementation and functional status of BDE. It shall be completed and provided to the COR no later than three days prior to the date the BEAP Steering Group convenes. The COR will provide comments no later than one day before the BEAP Steering Group convenes. The contractor shall incorporate any comments in time to provide the completed presentation to the BEAP Steering Group.

3.17 The contractor will provide and update technical documentation related to the following items on a quarterly basis with a final set of documentation due 11 months after award of the contract:

3.17.1 Technical notes relating to the design, implementation and development of the BDE system.

~~3.17.2 BDE System architecture and data models;~~

~~3.17.2 Transition plan that describes how the development system will be integrated and transitioned into production;~~

3.17.3 Out year Operation and Maintenance Plan (O&M) and forecast;

3.17.4 Development plan that can be used to guide future data source integration;

3.17.5 Interface control documents for system components and networks;

3.17.6 Documentation required to meet requirements set forth in DHS Management Directive 102 –01, Acquisition Management Directive, located at http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_102-01_acquisition_management_directive.pdf; and

3.17.7 Additional documentation as identified and required for OMB, FISMA and internal DHS government IT projects.

3.18 Briefing material, correspondence, memoranda. The contractor shall prepare on an as needed basis any briefing material, correspondence, and/or memoranda related to the BDE as requested by COR.

3.19 The contractor shall respond to any data calls as tasked by the COR.

3.20 At the end of the base period of performance, the contractor shall provide any work first produced such as configuration scripts, security scripts, software written, user manuals,

data models, interface control documents, user manuals, technical descriptions of the software and scripts, user operations manuals, system maintenance manuals, and anything else first produced under this contract.

IV. TASKS – OPTION PERIOD OF PERFORMANCE

The scope of work in the option year will add two additional domains within ICE/HSI and will build upon the work and deliverables in the base award. These two domains include ICE/HSI Support (Support) and the Cyber Crimes Center (C3). During the execution of the option period of performance, the contractor shall perform all of the same tasks as outlined in III.3.1 through III.3.20, as applied to both of the two new domains, Support and C3. In addition, the contractor is required to perform the following new additional tasks IV.4.1 – IV.4.6. Where noted below, however, some of the new tasks will modify or supersede existing tasks under III.3.1 – III.3.20.

4.1 Create Technical Baseline: The contractor shall develop a technical baseline of the current C3 and Support systems to identify system interfaces, protocols, and other detailed technical information that will enable integration with a) existing data sources, b) analytic tools currently used by HSI staff and/or third party tools that could be used in the future, and c) any other technical information relevant to implementation and integration. This task is applicable to both domains, Support and C3.

4.1.2 Create Requirements-Based Project Plan: The contractor shall create a project plan that details the development, integration, and organizational tasks necessary to achieve implementation in a way that meets the intent of the requirements. The project plan shall include schedule, milestones, and risks. This task supersedes task 3.13. This task is applicable to both domains, Support and C3.

4.1.3 Develop Proposed Architecture Document: The contractor shall provide a proposed technical architecture including any third party software as well as integration points with other necessary systems. The contractor shall make necessary adjustments to the architecture according to policy constraints and stakeholder needs. The contractor shall notify the Government of any conflicts or trade-offs between policy-constraints, stakeholder needs, and AIDW-BDE requirements. This task supersedes task 3.7.2 and 3.17.2. This task is applicable to both domains, Support and C3.

4.1.4 GFI, Approvals, & Stakeholder Map: The contractor shall develop a map of all the necessary approvals, government-furnished-information, and documentation that will be required for successful implementation. The map shall include the names and contact information of each stakeholder and their supervisor. The contractor shall develop simple communications materials explaining the development project, the approach, and what is needed from each stakeholder. This task is applicable to both domains, Support and C3.

4.1.5 Performance Metrics: Drawing on the C3 Enterprise Description, the contractor shall adopt or develop performance metrics for both the development process and the AIDW-BDE system performance. The contractor shall include progress against the development metrics in their monthly report. This task is applicable to the C3 domain.

4.1.6 Development Approach: The contractor shall devise a development approach aligned, where appropriate, with the agile development process. The contractor shall communicate that approach with the appropriate HSI staff, managers, and other enterprise stakeholders to prepare them for the required interactions and processes associate with Agile. The contractor shall develop an agreed-upon frequency and timeline for agile meetings where government personnel are required. This task is a continuation of task III.3.12. This task is applicable to both domains, Support and C3.

4.1.7 Reconfigure (e.g. increase and/or decrease the number of nodes) the cluster as part of supporting server configurations or virtual machines effectively and efficiently. This task is a continuation of task III.3.1.2. This task is applicable to both domains, Support and C3.

4.1.8 The contractor is required to provide a methodology and analytical approach for migrating the AIDW-BDE to a production environment at ICE. The contractor is expected to carry out the work required to migrate the AIDW-BDE system from a development and test system to a production system environment that is fully compliant with all ICE and DHS protocols such as FISMA, FIPS, DHS Privacy and other compliance standards. This task supersedes task III.3.3. This task is applicable to both domains, Support and C3.

4.1.9 Plugins: The contractor shall architect a system that allows for ad-hoc “plugins”-- lightweight locally scriptable modules that can automate the data processing needed by HSI AIDW-BDE users. This task is applicable to both domains, Support and C3.

4.1.10 Data-source & System Integration: The contractor shall integrate with all relevant data sources and systems that are not already integrated into the AIDW-BDE. AIDW-BDE interfaces with multiple systems and 3rd party software. The intent of this task is for the contractor to integrate with these systems. It is expected that this task will require significant organizational work in addition to technical work due to the system being connected across multiple agencies and different business units. This task is applicable to both domains, Support and C3.

4.1.11 Data analytics: The contractor shall implement analytic solutions that allow for both the application of analyst-generated rules as well as predictive analytic approaches. The data analytics capability should allow for high-performing queries, automated data evaluations and triage and system administration. Additionally, the analytics capability should provide for expert users to conduct complex analytic tasks across the entire data space in AIDW-BDE. This task is applicable to both domains, Support and C3.

4.1.12 User analysis tools: At a minimum, the contractor shall implement a) an analysis tool to enable analysts to conduct investigative analysis and b) a capability that allows analysts to create investigative workflows from rules they created. This task is applicable to both domains, Support and C3.

4.1.13 Data visualization: The contractor shall implement data visualization tools focused on key performance metrics designated by DHS S&T. Examples of performance metrics can be

found in ICE documentation. This task is applicable to C3 domain.

4.1.14 Design and implement ETL and data visualization tool to facilitate the analysis of documents related to the ICE/HSI Support mission. These documents will exist in a diverse set of file formats (PDF, etc). Examples of tools that may be employed for visualization include, but are not limited to, Elastic search/Kibana. This task is applicable to Support domain.

4.1.15 Workflow & communication: The contractor shall implement workflow and communication tools to help users track and document team communication and workflow management on referral candidates and specific referrals, including tools for easily generating referral reports based on the data tracked. This task is applicable to both domains, Support and C3.

4.1.16 Training: The contractor shall create a training plan that describes the user training approach, user guides and training sessions. User training will be conducted prior to and during transition. This task is applicable to both domains, Support and C3.

4.2 The contractor will be required to architect and model all data being uploaded into the AIDW-BDE system. This task supersedes task III.3.7. This task is applicable to both domains, Support and C3.

4.2.1 Creation of a data model for data sets that ICE intends to upload into AIDW-BDE to ensure accuracy when accessed by operational units at ICE. This task is applicable to both domains, Support and C3.

4.3 The contractor shall test, develop and integrate Extract, Transform and Load (ETL) tools into the AIDW-BDE system. This task is applicable to both domains, Support and C3.

4.4 The contractor shall support Test and Evaluation (T&E) activities carried out by ICE and DHS S&T for the AIDW-BDE system. This task supersedes task III.3.9. This task is applicable to both domains, Support and C3.

4.5 The contractor shall develop an interface between AIDW-BDE and data sources. This task supersedes task III.3.10. This task is applicable to both domains, Support and C3.

4.6 The contractor shall provide Database Administrator functions for the AIDW-BDE, and have the knowledge and ability to address any system outages or other discrepancies associated with the system. This task supersedes task III.3.11. This task is applicable to both domains, Support and C3.

V. DELIVERABLES

5.1 Base Period. The following table depicts the deliverables required during the base period of performance as a result of the tasks outlined above.

Deliverables/Key Milestones	SOW Paragraph	Due Date
Project Schedule	III.3.13	30 days after award
Technical Status Reports	III.3.14	Monthly, the 15 th of each month during the base period of performance
Financial Status Reports	III.3.15	Monthly, the 15 th of each month during the base period of performance
Presentation to the Joint Border Enforcement Analytics Program (BEAP) Steering Group	III.3.16	Quarterly as designated by the COR
Technical documentation outlined in III.3.17	III.3.17	Every three months after base award
Final set of technical documentation outlined in III.3.17	III.3.17	11 months after base award
Government review of BDE system documentation	III.3.17	11 months after base award
Final/revised BDE documentation	III.3.17	12 months after base award
Briefing material, correspondence, memoranda	III.3.18	As requested by the COR
Respond to data calls	III.3.19	As requested by the COR
All items first produced under the contract	III.3.20	At the end of the base performance period

5.2 Option Period. The following table depicts the deliverables required during the option period of performance as a result of the tasks outlined above.

Deliverables/Key Milestones	SOW Paragraph	Due Date
Project Schedule	III.3.13	30 days after exercise of option
Technical Status Reports	III.3.14	Monthly, the 15 th of each month during the option period of performance
Financial Status Reports	III.3.15	Monthly, the 15 th of each month during the option period of performance
Presentation to the Joint Border Enforcement Analytics Program (BEAP) Steering Group	III.3.16	Quarterly as designated by the COR
Technical documentation outlined in III.3.17 (except task 3.17.2)	III.3.17	Every three months after exercise of the option

Final set of technical documentation outlined in III.3.17 (except task 3.17.2)	III.3.17	11 months after exercise of the option
Government review of BDE system documentation (except task 3.17.2)	III.3.17	11 months after exercise of the option
Final/revised BDE documentation (except task 3.17.2)	III.3.17	12 months after exercise of the option
Briefing material, correspondence, memoranda	III.3.18	As requested by the COR
Respond to data calls	III.3.19	As requested by the COR
All items first produced under the contract	III.3.20	At the end of the option performance period
Technical Baseline	IV.4.1	1 month after exercise of the option
Project Plan	IV.4.1.2	45 days after exercise of the option
Proposed Architecture Plan	IV.4.1.3	45 days after exercise of the option
GFI, Approvals and Stakeholder Map	IV.4.1.4	45 days after exercise of the option
Test Plan	IV.4.1.2, 4.1.3-4.1.5	6 months after exercise of the option
AIDW-BDE cluster configured with all tools	IV.4.1.7-4.1.15	6 months after exercise of the option
Test Results	IV.4.1.2, 4.1.3-4.1.5	8 months after exercise of the option
AIDW-BDE optimized cluster delivered	IV.4.1.7-4.1.14	11 months after exercise of the option
User Training	IV.4.1.16	11 months after exercise of the option

VI. PERIOD OF PERFORMANCE

6.1 Base Period of Performance. As stated in section F.1 of the task order terms and conditions, the base period of performance is September 9, 2013 – September 8, 2014.

6.2 Option Period of Performance. As stated in section F.1 of the task order terms and conditions, the option period of performance September 9, 2014 – September 8, 2015

VII. PLACE OF PERFORMANCE

7.1 For development and testing, all work will be performed primarily at ICE at ICE Technical Operations in Lorton, VA. Some work may be performed at S&T Offices located at 1120 Vermont Ave, Washington DC on a temporary basis as determined by the CO/COR.

7.2 For production, work will be performed at an alternative ICE location. This location will be determined at a later date; however, the location will be in the National Capital Region.

VIII. TRAVEL

8.1 Travel is required in the performance of the work outline in this SOW. The Government will reimburse the Contractor for travel, as required, outside of the Washington DC area only. All costs associated with local travel within (50) mile radius of the Contractor's normal place of performance commuting area are not reimbursable.

8.1.1. Base Period of Performance Travel Requirements:

8.1.1.1. The Contractor shall send two people to visit the DHS – Northeastern University Center of Excellence ALERT (Awareness and Localization of Explosives-Related Threats) center in Boston, MA on a quarterly basis for a total of four trips.

8.1.1.2. The Contractor shall send two people to visit the NASA Stennis Space Center in Stennis Space Center, MS for a total of two trips.

8.1.1.3. The Contractor shall send one person to San Francisco, CA for a program related meeting for a total of one trip.

8.1.2. Option Period of Performance Travel Requirements:

8.1.2.1. The Contractor shall send two people to visit the DHS – Northeastern University Center of Excellence ALERT (Awareness and Localization of Explosives-Related Threats) center in Boston, MA on a quarterly basis for a total of four trips.

8.1.2.2. The Contractor shall send two people to visit the NASA Stennis Space Center in Stennis Space Center, MS for a total of two trips.

8.1.2.3. The Contractor shall send one person to San Francisco, CA for a program related meeting for a total of one trip.

8.2 The contractor shall request all travel in writing and provide the names of individuals traveling, dates, destination(s), purpose, and estimated costs. All travel is subject to advance government approval by the COR. Approval shall be provided in writing. Approved travel

outside of the defined local area will be reimbursed in accordance with the limits set forth in FAR Part 31.205-46 Travel Costs and the Federal Travel Regulations (FTR).

8.3 No profit is allowed for travel. Indirect costs may be applied to travel in accordance with the Offeror's established accounting practices consistent with FAR 31.2 Contracts with Commercial Organizations. Travel will be a separate not-to-exceed contract line item number on the task order. The travel costs will be minimized, to the maximum extent possible, by taking advantage of discounted airfare rates available through advance purchase. The Government will only pay travel expenses in accordance with FTR rates.

IX. GOVERNMENT-FURNISHED INFORMATION

9.1 DHS will provide access to Government information, equipment and materials as well as technical designs for the Contractor to support work included in this SOW. Such provided information, materials, and forms shall remain the property of the Government, unless otherwise indicated in writing by the Government, and may not be distributed beyond the Contractor's designated, cleared, and approved project Contractors without prior written permission from the COR.

9.2 The development & testing computing cluster and associated software will be available for the Contractor for use at the Government facilities.

X. GOVERNMENT-FURNISHED FACILITIES, SUPPLIES, and SERVICES

10.1 If work at government-provided facilities is necessary for the services being performed under this SOW, such facilities will be provided at S&T and ICE Offices identified in VII above. Parking facilities are not provided. Basic facilities such as work space and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general purpose office supplies) will be provided to contract personnel that are providing support at the designated facilities.

XI. SECURITY

11.1 DHS has determined that performance of the work included in this SOW will require the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) to have access to sensitive, but unclassified DHS information.

11.2 All sensitive, but unclassified, information shall be processed in accordance with **Management Directive 11042.1**, which is included as **Attachment J.4** of this award. This requires the Contractor to execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information.

11.3 During the performance of this contract, contractor assigned personnel shall have, at a minimum, an ICE Enter on Duty (EOD) qualification or an equivalent clearance from another DHS component.

11.4 Suitability Determination. DHS 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 background investigation. DHS may, as it deems appropriate, authorize and make a favorable expedited entry on duty (EOD) decision based on preliminary security checks. The expedited EOD decision will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract. No employee of the Contractor shall be allowed to EOD and/or access sensitive information or systems without a favorable EOD decision or suitability 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 EOD decision or suitability determination by the OPR-PSU. Contract employees are processed under the **DHS Management Directive 6-8.0**. The contractor shall comply with Homeland Security Acquisition Regulation (HSAR) 3052.204-71, Contractor Employee Access (SEP 2012) ALT I (SEP 2012), located in **section I.4.1.** of the contract terms and conditions.

11.5 Background Investigations.

11.5.1 Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, 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. Prospective contractor employees shall submit the following completed forms to the Personnel Security Unit through the COR, whether a replacement, addition, subcontractor employee, or vendor:

11.5.1.1 Standard Form 85P, “Questionnaire for Public Trust Positions” Form will be submitted via e-QIP (electronic Questionnaires for the Investigation Processing) (2 copies)

11.5.1.2 FD Form 258, “Fingerprint Card” (2 copies)

11.5.1.3 Foreign National Relatives or Associates Statement

11.5.1.4 DHS 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act”

11.5.1.5 Optional Form 306 Declaration for Federal Employment (applies to contractors as

well) Authorization for Release of Medical Information

11.5.2 Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

11.6 The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS IT systems and the information contained therein, to include, the development and / or maintenance of DHS IT systems; or access to information contained in and / or derived from any DHS IT system.

11.7 Transfers from Other DHS Contracts.

11.7.1 Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation an eQip Worksheet will be submitted to the Intake Team to initiate a new investigation.

11.7.2 Transfers will be submitted on the COR Transfer Form which will be provided by the Dallas PSU Office along with other forms and instructions.

11.8 Continued Eligibility.

11.8.1 If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

11.8.2 The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

11.8.3 The OPR-PSU may require reinvestigations when derogatory information is received and/or every 5 years.

11.9 DHS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

11.10 The contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COR. 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

employees' name and social security number, along with the adverse information being reported.

11.11 The OPR-PSU must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired DHS issued identification cards and building passes, or those of terminated 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.

11.12 Employment Eligibility.

11.12.1 The contractor shall agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

11.12.2 The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represents the best means currently available for employers to verify the work authorization of their employees.

11.12.3 The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

11.12.4 Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

11.13 Security Management

11.13.1 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.

11.13.2 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.

11.14 Computer Security. The following computer security requirements apply to both Department of Homeland Security (DHS) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

11.14.1 Information Technology Security Clearance.

11.14.1.1 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 IT Security Program Publication DHS MD 4300.Pub. or its replacement*. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

11.14.1.2 Contractors 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).

11.14.2 Information Technology Security Training and Oversight.

11.14.2.1 All contractor employees using Department automated systems or processing Department sensitive data will be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

11.14.2.2 Contractors 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 and systems rules of behavior. Department contractors, 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.

11.14.2.3 All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors 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).

XII. POINTS OF CONTACT

The points of contact (POCs) for this task order are as follows:

Contracting Officer's Representative (in accordance with **section G.1.2.** of the task order):

Department of Homeland Security

Task Order Award: HHSN316201200120W/HSHQDC-13-F-00123 (Proposed P00003)

Attachment J.1 – Statement of Work

Shane Cullen
U.S. Department of Homeland Security
Science and Technology Directorate/Innovation
Mailstop 0201
245 Murray Lane
Washington, DC 20528-0201
(202) 254-5679
shane.cullen@hq.dhs.gov

ICE Technical Representative:

Mr. Thariq Kara
U.S. Department of Homeland Security
Immigration and Customs Enforcement
Office of the Chief Information Officer
801 I Street, NW
Mail Stop 5808
Washington, DC 20536
(202) 732-3776
thariq.kara@ice.hq.dhs.gov

Contracting Officer (in accordance with **section G.2.2.** of the task order):

Linda Santiago
Contracting Officer
MGMT/OPO/S&TAD/Mailstop 0210
Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0210
(202) 254-6823
linda.santiagocaiced@hq.dhs.gov